Fostering Tools and Test Equipment for Smart Grid Interoperability

Rick Denker

Packet Plus, Inc.
Portland, Oregon 97201 USA

rick@pktplus.com

Keywords: interoperability, conformance, Ethernet, Wi-Fi, SNMP

Abstract

In creating a multi-vendor system that exhibits interoperability there is much more involved that just creating a detailed unambiguous specification. The current networking infrastructure exhibits a high degree of interoperability through a combination of several factors. This paper explains some of the lessons that can be learned from this previous networking industry experience.

A framework is proposed of technical specification, management process, support tools and market factors. The framework is then used to analyze four networking industry positive examples. The activities in each of the four areas of the framework will be described with emphasis on the key attribute that drove the interoperability. From these examples some of the specific techniques used will be described. Also the current reality of interoperability will be described.

Based on this information suggestions will be made on how to apply these lessons to the Smart Grid to foster better support tools. The ideas from this paper should help the Smart Grid industry to guide tool and test equipment vendors to better support them. It will help companies involved with the Smart Grid regarding information to provide tool and test equipment vendors and requests to make of tool and test equipment vendors.

1. HISTORY

Thirty years ago the computer world was much different. Most computers were stand-alone in a data center and few people interacted directly with them. The most common exchange issue was between EBCDIC and ASCII formats, and data exchange was achieved typically by walking the media (typically magnetic tape) from the drive on one computer to the next. Even as the world started to change with workstations and networks, the way communication between machines was actually achieved was often by purchasing all of the products from a single vendor.

However today it has evolved to a world where interoperability is imperative. The vast majority of electronic products now have features that are dependent on working smoothly and efficiently with products from other companies. The story of how the interoperability has actually been achieved is a complex mixture of many factors.

2. FRAMEWORK

The proposed framework states that getting to interoperability is made up of 1) technical specification, 2) ongoing management process, 3) supporting tools, and 4) market factors. Each is explained briefly, and will become clearer as they are applied to the case studies. These attributes are not presented in a particular order, since the importance varies from standard to standard. Often one attribute will swamp all the others for a period of time. However, the most robust and enduring situations where interoperability is achieved has been a combination of more than one of the attributes.

2.1. Technical Specification

A complete and unambiguous technical specification plays an important foundation in creating interoperability. Getting all the companies involved in an industry standard to “fly in formation” is a difficult technical task. Even with well written specifications the differing interpretations can cause lack of interoperability, or the creation of industry cliques.

However, often the market reality is not reflected in the technical specification. There are several cases where if you follow the technical specification you will not work with any other equipment. This can happen when the standard is not clear, or when companies were required to make product decisions before a standard becomes final. If the initial mover gains a large share, it is common this becomes the default specification for the market.

2.2. Supporting Tools

The tools that are used in development and testing provide an important component in creating interoperability. They can be critical to measuring the adherence to the technical standard or the tracking down any discrepancies. Without strong measurement tools the variance between vendors can become quite large.

2.3. Management Process

The ongoing process around a standard is very important. This includes the standards group, forums for companies to communicate their interests, the method for deciding and communicating changes, and the product certification process. There is often a political process for determining the interests of the companies involved. Therefore a known process that companies are familiar with can be a benefit to keeping the politics manageable.

2.4. Market factors

Several market conditions play a role in interoperability, including the speed of adoption, the relative market share of key players, and the effect of related markets. For example, a market with a dominant player may use a standard to spread their influence. Alternatively, a standard may be the way that several smaller players work against a larger player. These forces cannot be ignored and are often a major influence in how interoperability actually plays out.

3. CASE STUDY: ETHERNET

Ethernet started as a technology developed at Xerox PARC in the mid-1970s, then pushed for broader adoption by corporate supporters (DEC, Intel, Xerox) in the early 1980s. It became the first local area networking standard with broad adoption. It has undergone several metamorphoses through the years, from coaxial cable to twisted pair, and from 3 Mbits/s to multi-Gigabit/s. It now provides the basis for most commercial LANs.

3.1. Technical specification

The technical standard is now managed by the Institute of Electrical and Electronics Engineers (IEEE) (802.3). The technical specification is well developed. However, equipment manufacturers still have to sort out the realities. There are still cases where strictly implementing the standard will lead to not working with other equipment. Companies are required to develop this inside knowledge. There are also many cases where manufacturers do not implement 100% of the specification. So equipment will interoperate most of the time, but there will be exceptions for particular features.

3.2. Management Process

The IEEE manages the input and modification process for the specification. The Ethernet Alliance is primarily a promotion vehicle for Ethernet adoption. It does organize plugfests for new areas of the standard, but does not provide certification.

3.3. Support tools

The loading and test tools from Spirent, Ixia, and Agilent, have been the dominant force in creating interoperability. These testers provided a coordinated conformance test. They provide engineered traffic on all ports of a piece of equipment in a precise and repeatable way. They provide a convenient and consistent way to set up a test configuration for quality assurance applications.

Passing the SmartBits® or equivalent test has become an imperative for anyone building an Ethernet chipset. Every packet dropped in the test must be explained with plans for the correction in a future version of silicon. This has fostered an industry where there is little variance on the parameters that are key for interoperability.

3.4. Market factors

The market for Ethernet PHY (physical interface) chips has been well developed with a couple of significant players. This has lead to the broad knowledge in how the two players products worked and the quirks of how they work. The interoperability challenges have migrated up the stack to layer 2 and layer 3.

3.5. Summary

The rigorous testing tools are the driving force in creating the broad interoperability of Ethernet.

4. CASE STUDY: WI-FI®

Wireless networking using unlicensed spectrum first came to market in the early 1990s and became standardized as IEEE 802.11. The standard is often referred to as the "wireless Ethernet". It experienced explosive growth in the middle of this decade when it started being included in laptop computers. It also had major crisis when the weakness of the Wired Equivalent Privacy (WEP) encryption was exposed and threatened to give it a blackeye on security. This prompted a flurry of activity to quickly implement a stronger security version, called Wi-Fi Protected Access (WPA)®.

4.1. Technical specification

The technical specification like Ethernet is managed by the IEEE (802.11). The specification has benefited from the experience of Ethernet. However, there is the additional complication of the radio. The modulation method has continued to become more complex as the standard works to develop faster speed standards that exhibit reasonable resistance to interference.

4.2. Management Process

The Wi-Fi Alliance (WFA) has played a key role. It offers an extensive certification program that checks that a piece of equipment works at an acceptable throughput level with four pre-determined vendors' equipment. They also provide certification of other specific advanced features. Passing the certification was a requirement for a piece of equipment displaying the Wi-Fi® logo.

When the security issues with WEP occurred the WFA stepped up to the plate providing the group communication, being the standards body, and providing the certification for a quicker response to the issue than could be completed through the IEEE.

The certification processes of the WFA were put in place when there was wide variance in products, and customer skepticism. Now there is broad interoperability.

4.3. Support tools

The pervasive tools for Wi-Fi were protocol analyzers and IxChariot from Ixia. The protocol analyzers provided a symbolic decode of traffic logs, and Chariot provided an application level loading tool. However, these initial tools could not measure certain details of the standard. For example testing if an acknowledgement was within the window specified by the standard was not possible until the VeriWave test tools with more precise timing measurement were introduced.

When applications such as Voice over Wi-Fi (VoWiFi) become predominant the precise measurement of VeriWave tools may become critical for interoperability.

4.4. Market factors

The logo program on the WFA created an easy and visible way for customers to know that a device had been certified. Being certified became a market requirement for chipset and equipment vendors.

Cisco has a large market share in wireless access points. They made the decision to focus on access points and promote their own certification program for client devices.

Also products are differentiated on the range and resistance to interference capabilities of their radio, because of this there has not been a consolidation of radios used for Wi-Fi. This has forced the need for more physical layer testing, than is true for Ethernet.

4.5. Summary

The strong process of the Wi-Fi Alliance has been the driving force creating the broad interoperability of Wi-Fi. In the future this may evolve to more test equipment based as the standard and application requirements become more stringent.

5. CASE STUDY: SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

SNMP is used to monitor devices in a network for conditions that warrant management attention. Each network device has a unique set of conditions that need to be monitored. Therefore each networking equipment design must create a unique implementation that works with the standard. SNMP has benefited by being the standard in place when the Internet took off, and it is even more entrenched now.

5.1. Technical specification

SNMP is a component of the Internet Protocols Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of related standards that includes an application layer protocol, a database schema, and a set of database objects.

The initial standard was developed by people that were knowledgeable in the realities of building networking equipment. This ensured that the standard was practical and implementable. In addition to this there were reference implementations that were available initially, both in the form of commercial reference platforms, and open source versions. With this leg up provided almost all implementations started from this common core ancestry. This drastically increased the chances of successful interoperation.

5.2. Management Process

The Internet Engineering Task Force (IETF) provides the coordination and communication of the standard. There is not a certification process for vendors. In the early years of the standard there were some plugfests that were organized on an ad hoc basis. However, there is not an ongoing organized meeting to test interoperability.

5.3. Support tools

The standard works above the physical layer, so no PHY or link layer measurement is required. The tools that are used are just the network management tools that use the SNMP data. There have been some commercial testing tools, but they have not gotten any broad acceptance.

5.4. Market factors

Many vendors provide network management software with no one dominat market player. SNMP Research is a third party supplier that provides SNMP support for a broad set of manufacturers, increasing the chance of interoperability.

5.5. Summary

The strong and flexible standard combined with the extremely complete specification has been the key to the broad interoperability of SNMP. This combined with the pressure on each equipment vendor to make sure that their equipment is well supported has led to perhaps the broadest interoperability of any networking standard.

6. CASE STUDY: MICROSOFT PLUG-AND-PLAY DRIVERS

Historically when interfacing to a new hardware device the user would have to set a jumper or set a DIP switch on the hardware. These were often problematic, when the jumper was misplaced, or the switch incorrectly set. As computers became more broadly used this put tremendous pressure to create a better solution.

The solution plug and play drivers where the discovery of a new hardware component in the system happens automatically. This hides the complexity of the equipment configuration and interaction from the user. To ensure that the user has a positive experience with their operating system, Microsoft takes on additional support and verification tasks.

6.1. Technical specification

Microsoft provides equipment makers with the specification for developing software drivers. Because a single company controls the specification it makes the resolution of interoperability issues quick and allows quick response to major issues.

6.2. Management Process

Microsoft certifies drivers to be included with their distributions. The equipment vendor provides the hardware and driver to Microsoft. Microsoft has a dedicated team that certifies the hardware and associated driver. This provides a consistent review of the functionality and keeps the knowledge within one company from release to release.

6.3. Support tools

There are no particular third party tools involved in making interoperability happen. However, the hardware providers will often provide additional access that is not documented. They will provide this information to Microsoft, for support purposes and during the verification process.

6.4. Market Factors

Microsoft's dominant market position in operating system software makes it imperative that equipment providers fit into the Microsoft framework. Microsoft is also pressured to ensure the users have a positive experience with their operating system.

6.5. Summary

It is Microsoft's market position that allows them create the system that creates the high level of interoperability. It is the structure that they put in place to support specification, certification and support that makes it work.

7. TECHNIQUES

There are several techniques that are used to foster interoperability. Below is a list of several of the more popular techniques.

7.1. Engineered Corner cases

Corner cased are effective because they put extreme stress on a system, even more than would ever occur in normal operation. An example would be to run minimum sized packet back to back with a minimum inter-frame gap at full protocol rate. This gives the equipment the minimum time to process the traffic. Often quality assurance (QA) departments use specialized test equipment that can generate this traffic on every port of the device in a way that is time synchronized to be repeatable. This level of testing will both improve interoperability and increase the robustness of the system.

7.2. Short controlled interactions tool

Interoperability is made up of thousands of small interactions working properly. One of the key tools to accomplish this is a flexible and controllable traffic generator. The purpose is to create small, usually just a few packets, test cases. These test snippets can be used as part of a larger certification test, or to debug a situation where two pieces of equipment are not working together.

These are often custom tools that each equipment maker develops. For the Wi-Fi standard a chip maker developed a java-based scripting tool that was broadly used. There may need to be different tools depending on the layer of the stack that is being tested. There is an open source tool called SCAPY that can be useful for this task.

7.3. Automated regression testing

Keeping track of the thousands of tests is a daunting task. It also becomes very error prone if it is not automated. This is especially true when issues such as backward compatibility are considered. The logistics of this can become quite complicated when issues such as physical location or resistance to interference need to be considered. In wired standards such as Ethernet the testing of the physical media can be easily separated from the testing of the higher protocol without any concerns. However, for Wi-Fi where features such as roaming are a critical part of interoperability this becomes quite complex.

7.4. Alignment with standards group

Many standards that started by companies have migrated to be managed by standards groups. Ethernet and Wi-Fi are just two prominent examples of this that are managed by the IEEE. The standards group provide procedures for communication, upgrade process, that are critical for the continued success of a standard.

Many companies are already familiar with the procedures and are comfortable with their stewardship. However, it is important to consider the costs involved for each company. These may create an unwanted burden for some. Also the responsiveness of a standards group can be critical. These groups manage the input from many companies, but this can lead to being slow to respond to crisis. For example, the Wi-Fi Alliance took control of the response to the WEP security issue that threatened the enterprise acceptance of Wi-Fi.

7.5. Reference Designs

An example implementation that can be used as a reference can go a long way to creating interoperability. This can be done as a working reference that developers have access to, or as an open source implementation, where all the details are exposed. This can allow developers to view one possible implementation, run their design against the reference, and test specification ambiguities.

7.6. Certification process

Some standards have a formal certification process. For example, Wi-Fi has a formal set of tests that must be passed to allow a piece of equipment to exhibit the Wi-Fi logo. They have different certifications for different versions and features of the standard. Equipment providers pay a fee for their equipment to be tested, to cover the expenses. In the Wi-Fi case the submitted piece of equipment must meet an acceptable throughput rate with four different vendors' equipment. In setting up a certification process there are many questions about the process that need to be answered, including staffing and access to the certification labs, selection of the "gold" vendor units, and the location of labs.

7.7. Plugfests

Meeting of equipment providers for the purpose of checking out interoperability are commonly called "plugfests", because the vendors are continually plugging different combinations of equipment together. Each vendor brings the equipment that they want to test along with experts on those products. They are often located at testing labs, so that other infrastructure such as test equipment is readily available. These can be quite productive in highlighting issues between vendors. They can be critical for cases where none of the equipment is on the market yet, and provide productivity gains versus meeting with each individual vendor separately.

7.8. Testing labs

There are several testing labs that offer services that are useful for interoperability. These labs provide the resources of a knowledgeable staff, test equipment, and physical location. Some testing labs become aligned with certain standards for certification services. This provides efficiencies for the standards, since they do not need to duplicate the resources for their standard, and are often ideal in the early stages of a standard when this overhead would be a burden.

Of special note is the University of New Hampshire Interoperability Lab (UNH-IOL). It is the largest and most influential lab regarding networking interoperability. It is structured as a collection of consortiums for different standards. For each standard a company pays a membership fee to belong. As a member they are required to keep working copies of their equipment at the lab. This creates a critical mass of knowledge and equipment that makes the lab a popular location for plugfests.

8. THE REALITIES OF INTEROPERABILITY

It is important to consider the limits of what can be created in terms of interoperability. Getting to 100 percent interoperable is a good goal, but often hard or too expensive to reach in reality. This section discusses some of the realities that should be considered.

8.1. You often cannot strictly follow the written specification

There are many specifications where if you follow them to the letter, you have a good chance of not working with any other equipment. There may have been a divergence from the specification and it was not determined that making the two match was worth the cost and effort. Many equipment vendors view this as a cost of doing business and actually prefer this as a barrier to new entrants. To enter the market you may be forced to use a testing lab, or hire personnel that are knowledgeable in the realities.

As an equipment developer you may be presented with the dilemma of following the standard or actually being interoperable. In these cases the choice of actually being interoperable almost always wins. It can be even more difficult when in the market reality there are multiple working implementations in the customer base.

8.2. Even "certified" products may still have some issues

Although products that have been certified are much more likely to be interoperable, there are still exceptions. These

can come from three main sources. First, there are gaps in the completeness of testing. The test and measurement vendors are continually striving to match the "real world" situations of networks. Second, the combinatorial explosion in testing with every other vendor becomes unwieldy. Certification processes are forced to make an economic decision on the amount of coverage in the testing. And third, products and networks are not static. An upgrade to a feature, or using a new source for a component can introduce new issues.

8.3. Even if you follow the standard the other guy might not

It can be very hard to distinguish which piece of equipment is at fault. The customer may be angry with you even when you are doing it right. This is where efficient controlled probing tools can be invaluable to settling the issue. At least you may be able to give the other guy the "black eye", and explain the details to the frustrated customer.

9. APPLYING LESSONS TO PROMOTE BETTER TOOLS

There are many logistical decisions to be made regarding how to create the desired interoperability. Many of these decisions will focus on what part of the process needs to be shared or centralized between vendors, and which part is the responsibility of each individual vendor. Hopefully, the prior discussion and case studies will foster broader thinking and a search for the right examples.

Instead of attempting to give general advice, in this section of the paper will focus on steps that can improve the ability of tool vendors to provide strong support. First the major aspects that promote equipment interoperability are good for test equipment also. So create clear, complete technical specifications, set up an ongoing management process for communication (meetings, updates), and make sure there are reasonable financial incentives for building tools. Next consider the following four points.

9.1. Conformance versus interoperability

The decision that has the biggest impact on support tools is the choice between conformance testing versus interaction testing. Both methods can produce good results, but they have different trade-offs. The kinds of support tools required are dramatically different. A formal analysis of the two different techniques is provided in a Grid Interop 2008 paper [1].

Conformance testing means extensive checks on all of the parameters of the standard. This implies the creation of testing equipment that can measure all the parameters. This can be an expensive development and may need to be seeded initially to make it financially feasible. Once the test equipment is completed it drastically simplifies the logistics of certification testing. Each piece of equipment to be certified just needs to be measured with the test equipment. Depending on the cost of the equipment, it may be possible for all interested companies to have a tester. For each revision of the standard the test equipment must also be upgraded.

Interaction testing means connecting two or more of the pieces of equipment together and then checking that they interoperate successfully. This typically involves 1) reference units, 2) known traffic or load for the system, and 3) reference behaviors to verify. The reference units are known good equipment that all the other equipment must work with. The traffic load is an application that can be run on the equipment that simulates the conditions of operation in a network. The reference behaviors may be a measurement such as a throughput measure (packets/sec) or a functional result such as traffic rejected. Interaction testing typically is less expensive, but can have difficulties with "chicken/egg" dependencies and equipment logistics.

9.2. Levels of testing

The next biggest impact decision for support tools is what levels the testing will be required, and the interaction between the levels. The kinds of tools to measure the physical layer (spectrum analyzers, or reflectometers) are very different than tools that are higher up the stack (protocol analyzers, traffic generators) or application level tools (software loading, network monitoring). Having tools at all levels may prove to be too expensive, and decisions will need to be made regarding which levels are the most critical.

Another aspect of this is deciding whether the tests at different levels are independent of each other. If the levels are dependent on each other then the testing between the levels will need to be coordinated creating complex test equipment set up and coordination. An example of testing that can be independent is the physical layer from upper layers of Ethernet. An example of testing that is dependent is roaming behavior in Wi-Fi. Here the ability to detect the proximity to an access point (a physical layer measurement) directly affects the higher level protocol behavior.

9.3. Create standard user profiles

Information that can help create better support tools is the profile of system users. To make the profiles as close to real as possible, it may be worth conducting market research to determine the characteristics of users, and the portion of the overall population that they represent.

This information can drive traffic generation tools, determine the parameters for capacity testing, and provide system planning tools. With the profiles tools can create "dummy" users that can be easily created in specified quantities to simulate system loading. This can be useful to make sure that system data structures are efficient enough when their size gets large. Also being able to estimate the performance impact when adding a hundred new users can help drive decisions on when to upgrade a piece of equipment.

9.4. Develop Corner Cases

Corner cases can provide an efficient method for creating tests. Often when the corner cases are properly handled, then the general cases are handled too. So by creating a set of the important corner cases it can provide enough coverage that exhaustive testing may not be required.

The cases will vary from standard to standard depending on the goals of the end system. The corner cases can be in many different varieties. They can be an action (add a user, complete a transaction), a performance measurement (packets per second), an engineered situation (continuous back to back packets), a critical timing of an event (recovery, switchover to a new price, time change), or a user perceived value (response time). Corner cases can also deal with making sure that incorrect input is properly handled, so it could be input that includes errors, or even input that is attacking the security of the system.

The specific corner cases can then be combined together, or combined with the loading of different size user configurations for a more complete test.

10. CONCLUSIONS

Creating interoperability in practice involves a combination of the four factors of: technical specification, building an ongoing management process, support tools and market factors.

Different standards have achieved broad interoperability in distinctly different ways as shown by the examples of Ethernet, Wi-Fi, SNMP, and Microsoft plug and play drivers.

A list of possible techniques to foster interoperability was generated as a method to create ideas.

Specific suggestions on how to foster better support tools were made:

Decision of conformance versus inter-operation
Decision on levels of testing and whether they can be independent of each other
Creating user profiles
Building representative corner cases

10.1. References

[1] Drummond, Rik, "The Probabilistic Correctness of Conformance and Interoperability Testing" Grid-Interop 2008, pages C12-C21.

Biography

Rick Denker, CEO, Packet Plus, Inc.

Rick has over 25 years experience in high technology product marketing and business development involved with products for engineers.

Rick is the founder and CEO of Packet Plus. Packet Plus is building a next generation tool for the networking equipment development engineer, hardware or software. It goes beyond current custom tools by lowering development costs, increasing developer productivity, and improving re-use. A patent is pending on the concept.

Rick was co-founder and Vice-President of Marketing for VeriWave, a wireless LAN test equipment company. He participated in the Wi-Fi Alliance process for developing a test for Voice over Wi-Fi, and the IEEE standards group on how to test Wi-Fi. As a marketing manager for PMC-Sierra, he developed tool partnerships and launched an Ethernet chipset.

Previously Rick has worked for Palm, Synopsys, and Hewlett-Packard.

Rick has a Master of Business Administration degree from the Amos Tuck School at Dartmouth College, and a Bachelor of Science degree in Computer Science and Engineering from the Massachusetts Institute of Technology.