ECFS - E-mail Filing
<PROCEEDING>   09-31 (says 09-51 internally)
<DATE>   30 June 2009
<NAME>   Rex Buddenberg
<ADDRESS1>   2151 Trapani Circle
<ADDRESS2>
<CITY>   Monterey
<STATE>   Ca
<ZIP>   93940
<LAW-FIRM>
<ATTORNEY>
<FILE-NUMBER>
<DOCUMENT-TYPE> COmment
<PHONE-NUMBER>   831/646-9876
<DESCRIPTION>   Comment
<CONTACT-EMAIL> buddenr21@comcast.net
<TEXT>

From : Rex Buddenberg

To: Federal Communications Commission

Reference: GN Docket No. 09-51[1], National Broadband Plan

Point of view (14) and (72))[2]. I am writing this as a private citizen. But my viewpoint is from that of providing interoperable communications for emergency services.

Reasoning. Supporting emergency services properly will overtake the needs of a great many other claimants, both government and non-government under this legislation and subsequent plan. For example, emergency services need communications coverage throughout an area, including rural areas – complementing, but exceeding, the USDA Rural Utilities Service requirements. Similarly, every place that the school system needs internet, the emergency services providers need it too; the emergency services requirements consistently are a superset of school ones.

Responding to specific comment requests.

(15). "Broadband can be defined in myriad ways." Recommend you go behind the definition to intent. The stated requirement should be to 'extend the internet'. In the case of emergency services, this means 'extend the internet to mobile platforms' such as fire trucks, ambulances and police cars. Also in the case of emergency services, we should fix the intent as 'extend the internet to reach to the citizenry served', whether they are mobile (e.g. in automobiles) or not (at home, or work, or school).

The meta observation here is that regardless of the definition of 'broadband' all candidate technologies are packet switched ones – they can be used to extend the internet. By contrast, those technologies that are generally classed outside of the foggy definition of broadband are circuit-switched ones. Recommend that you consider replacing 'broadband' with 'packet switched' or 'routable network segment' – terms that clearly connote extending the internet.

(16) and (44). For the FCC's historical spectrum management purposes, 'broadband' can be interpreted to mean that spectrum should be allocated in MHz-sized slabs rather than KHz-sized slivers[3]. In the emergency services world, much of the existing spectrum allocations are in 25KHz, 12.5KHz or 5KHz slivers which inhibits using these bands for technologies like WiMAX or LTE. There may be other technologies than these candidates, but they can be expected to need MHz sized spectrum allocations and time-slice their subscriber stations (packet switching vice circuit switching)[4]. From a larger internetworking perspective, any technology considered as a candidate should come in the form of routable network. A routable network can be described as a communications cloud surrounded by routers; and is agnostic about the specific technology inside the cloud. Recommend that your Plan

1 The page header says 09-31; the first page heading says 09-51. In any event, National Broadband Plan is what I and commenting on.

2 The parenthetical paragraph numbers are those in your GN Docket No. 09-51 NOI.

3 The antonym of broadband in this context would be narrowband

4 Observe how IEEE 802.11/WiFi uses the 2.4GHz uinlicensed spectrum. While WiFi is unsuitable as a radio-WAN (because of it's non-stable MAC), the spectrum usage is 'broadband' in the same sense that IEEE 802.16 and LTE implementations would be.

require routable networks ubiquitously and to allocate spectrum in MHz-sized slabs..

(16). "Are there specific Commission actions that could encourage more rapid adoption of these more advanced broadband deployments... ?" There certainly are. The Department of Homeland Security's web pages providing grant guidance to emergency services are all written with narrowband (e.g. P25 and otherwise circuit-switched) technology in mind and are inconsistent with the expressed goals of this NOI. Whatever your definition of broadband, the DHS grant guidance is not. Recommend getting the entire federal government onto the same track.

(17) and (18). For emergency services, attempting to define 'broadband' by capacity is an irrelevant metric. The defining metrics for emergency services are

- Communications interoperability = internetworkability (see (15) above)[5].
- Geographic overage. Particularly important for rural reach.
- Availability. Defined as up time / total time. Most emergency services require at least Ao=0.999 which routinely forces multiple-threaded communications systems that can function by working around a piece of broken equipment, and decouple repair time from restoral time.

(19) and (46). Do not recommend fixing on a specific technology; this both tends to lock technology in amber, inhibiting innovation, and tends to unnecessarily bias one industry against another in an unwarranted fashion. It also tends to bias providers to deploying radio-based broadband solutions in situations where cabled broadband solutions are a better (and more spectrum efficient) local choice. Rather, recommend fixing on an internet-based modularity model and allowing alternatives within. After all, the internet is made up of multiple routable networks ... of several different specific technologies. The interoperability and performance requirements:

One. Any candidate technology must come in the form of a routable network (see (15) above).

Two. Any radio-WAN candidate technology must exhibit these properties:

A. a stable media access controller (MAC) that will not stall when overloaded with too many subscribers with too much data.

B. ability to support point-to-multipoint. Emergency services data contains a much higher proportion of data that is multicast in nature that civilian applications.

C. some reasonable infrastructure protection mechanisms necessary to prevent denial of service and theft of service attacks. (see my comment to (58) below – user privacy/authenticity requirements are NOT the ones we need here).

Three. The third principle of high availability engineering is prompt detection of failures. So any candidate technology should have a Simple Network Management Protocol agent in equipment for that purpose (see comment to (94) below).

Recommend: Your National Broadband Plan should indeed encompass radio technologies, but should emphasize a wired internet foundation on which to place the reach to mobile.

(40) and (41) and (52) and (72). For most areas of the United States (other than possibly urban ones), it is uneconomic to support an emergency services broadband infrastructure and a separate commercial

5 'Interoperability' is a term as devoid of precise definition as 'broadband'. For purposes of this inquiry 'interoperability' should be scope-limited to 'communications interoperability' and equated with 'internetworkability'.

(or non-EMS government) broadband infrastructure. Further, it is equally uneconomic to support separate broadband infrastructures for emergency services and for schools -- funded from the same tax base at the county level.

By the time the emergency services high availability needs are accounted for, most of the school requirements are exceeded. Further, schools have our children – a Number One priority concern in a disaster, and many schools have emergency services requirements (e.g. refugee center) in their own right. Recommend that a broadband plan foster unification of the treatment of these requirements.

What makes more sense is for a Wireless ISP to provide for the emergency services requirements and the school requirements (with appropriate subsidies and anchor tenant agreements) and then be allowed to sell the capacity beyond what emergency services and schools are using commercially.

(53). We should note how civilian consumers are using 'wired broadband' (e.g. DOCSIS and DSL) in residences today. The cable companies' vision a decade ago was to reach to a single end system in residence; but most users have purchased low-cost routers and have a LAN (either wired ethernet or WiFi) in their residence with several end systems attached.

This model pertains to emergency services as well. One use case would be an ambulance that has a radio-WAN[6] reach to the ambulance, to a router, and to a LAN with several medical diagnostic machines on that LAN. Another use case might be a fire truck with a radio-WAN reach to a router on the truck and a WiFi 'splotch' to support both local and reachback communications from the fire location. Few emergency services organizations seem to yet understand this blossoming, but it will assuredly happen and your plan should not inhibit that.

(58) and (73) and (75). The general subject of security requires a more detailed treatment because of the potential for trying to solve data protection problems with infrastructure protection tools – an impossibility metaphorically akin to sawing wood with a screwdriver.

Note that privacy (58) is properly a function of the data, not the infrastructure and it applies end-to-end across multiple network segments. Further note that membership on the internet conveys no assumptions about authenticity. Universal, ubiquitous authenticity is required; particularly on all '911' type of information transfers. Also end-to-end across multiple network segments. Emergency services data, especially including '911' type should, without exception, be authenticated (75). Authenticity and confidentiality are both properties of the data, not the infrastructure transporting it.

The IEEE 802.16 (WiMAX) and LTE and DOCSIS standards cover layers 1 and 2 of the ISO Reference Model and are scope-limited to a single network segment. So any security measures appropriate to those technologies are equally scope-limited. It is impossible to provide end-to-end security from this point – all security measures specific to a network segment technology must be reversed before datagrams are passed to a router.

Privacy (confidentiality) and authenticity concerns are end-to-end issues and cannot therefore be effectively addressed with link-layer technologies. Rather end-to-end security solutions are the only feasible ones. The internet SMTP/S/MIME standards that include mechanisms for both digital signature and encryption of e-mail body parts are a good example of protecting the data end-to-end (and remaining agnostic about the infrastructure).

The peril is that 'broadband plan' – the subject of your NOI -- implies layer 1 and 2 solutions – infrastructure such as DOCSIS, WiMAX and LTE. Which are inappropriate places to pursue privacy

6 WLAN – wireless LAN means reach from last router to end systems ... at the fringe of the internet. I'm using the term radio-WAN to denote router-router interconnect – in the interior of the internet – end systems are on the other side of the ambulance's router.

and authenticity solutions. Indeed it's difficult to see where security improvements over what is already in these standards will benefit us much.

Recommend. If privacy and authenticity are part of the national broadband plan, and not simply ruled out of scope, then the plan should include ISO Reference Model layer 6 and 7 solutions that are improvements of the protocol stacks in computer operating systems and their attendant applications[7].

(94). A thesis that I advised a few years ago uncovered that there are three major categories of IT infrastructure support tasks:

- Network operations. This is a watchstanding (24/7) function of making sure the internetwork continues to function – fault monitoring, trouble ticket operation, tech control. It is the human dimension to (19) Three above.
- System administration. This is a dayworking function.
- An unnamed category that includes 'install, configure, troubleshoot' tasks; also a dayworking function.

My thesis student found that these functions consistently appeared in both military and civilian situations and in both data center and internet service provider contexts.

We also found that the apprentice and journeyman level requirements for these skills can be taught in high school and junior college (and as military occupational specialty schools, known in the Navy as A schools).

But this training does not seem to have penetrated into our vocational educational system. If we are going to implement a national broadband plan, then we need the body of skillsets necessary to support it in our workforce. Recommend that the Plan include vocational training development in these categories for high schools and junior colleges.

In conclusion, recommend that the National Broadband Plan focus on extending the internet both to 1) emergency services mobile platforms and 2) to the citizenry for emergency services purposes.

This extension of the internet should and can be done in an 'open' fashion that does not inhibit the commercial use nor does it inhibit any of the worthy subsidiary uses (e.g. education, extended health care ...) mentioned in your NOI. The emergency services requirements should be placed at or near the top of the priority list because meeting these needs will overtake many of the other concerns your inquiry has posed.

7 Recommend consider the Common Alerting Protocol work as foundation for this subject area. http://www.oasis-open.org/specs/