Independent Submission
Request for Comments: 6217
Category: Experimental
ISSN: 2070-1721

T. Ritter

1 April 2011

Regional Broadcast Using an Atmospheric Link Layer

Abstract

Broadcasting is a technology that has been largely discarded in favor of technologies like multicast. This document builds on RFC 919 and describes a more efficient routing mechanism for broadcast packets destined for multiple Local Area Networks (LANs) or Metropolitan Area Networks (MANs) using an alternative link layer. It significantly reduces congestion on network equipment and does not require additional physical infrastructure investment.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6217.

Table of Contents

1. Introduction

RFC 919 [1] defines a method for broadcasting packets to a local network. It assumes that data link layers support efficient broadcasting. In the years since RFC 919 was written, Local Area Networks have grown exponentially in size, and frequently they are not geographically local.

This RFC proposes a new data link layer that scales efficiently to a geographically local network and, depending on visibility, to an entire Metropolitan Area Network. By using a different transmission medium, the broadcast traffic does not impact current inter- or intra-network routed traffic. It also makes use of a widely available infrastructure that is in use in all major cities and, surprisingly, rural and under-developed locations as well.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

3. Limitations

This RFC does not propose solutions to all problems. Just as RFC 919 was unconcerned with reliability, we also do not guarantee that hosts receive datagrams sent. Hosts may not receive packets for a variety of reasons, among them weather conditions, line of sight, sleep patterns, and distraction. A best-effort delivery approach is taken.

These limitations do impact the usefulness of the proposal, but organizations serious about distributing information in this fashion can overcome these obstacles with relatively little difficulty.

4. Physical Layer

The physical layer used is made up primarily of nitrogen and oxygen, at a pressure of 101.3 kilopascal at sea level, but dropping to about half that pressure at operating altitudes. Microscopic residue or trace elements may exist in the transmission medium, depending on local formation properties.

This residue may include argon, carbon dioxide, neon, helium, chloride anions, sulfur dioxide, and other molecules occurring at very low mixtures. It is common for there to be some degree of gaseous dihydrogen monoxide present. These trace molecules usually do not impede the broadcast, although further details on datagram transmission follow.

5. Frame Format in the OSI Model

It is always a challenge to design a protocol that allows enough flexibility for future adaptation while keeping it efficient in size -- and for this medium, size and complexity of the header are of particular concern. For this reason, this RFC proposes recommendations for the Data Link, Network, and Transport Layers.

Implementations MAY use any protocol that fits their needs for the Network and Transport Layers. They SHOULD consider how different protocols may be interpreted by recipients of the message and choose the most effective protocol available. The protocols defined have been designed to allow maximum ease of interpretation, so their use is encouraged.

5.1. Data Link Layer

The Data Link Layer is primarily concerned with transmitting datagrams between adjacent nodes, and it is unnecessary here since we only support broadcast transmission. Implementers MUST NOT encapsulate packets in a link layer protocol.

5.2. Network Layer

When designing a protocol for the Network Layer, it makes sense to consider existing protocols in this layer and reference their strengths and weaknesses. Looking at IPv4/6, we can see their header structures include several fields unnecessary for our purposes:

Destination, TTL (Time to Live), DSCP (Diffserv Code Point), ECN (Explicit Congestion Notification), Hop Limits, and so on. We can design a much more compact protocol thusly:

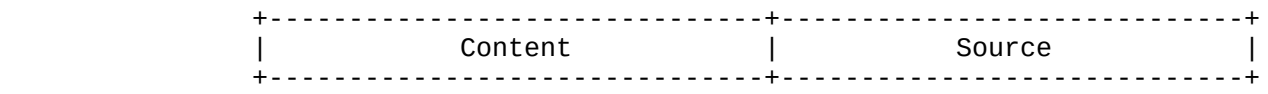

Figure 1: Layout of the Datagram

Content - A variable-length field containing the encapsulation of higher-level protocols.

Source - The sender of the message. A transmission MUST choose one of the following representations of the source:
- IPv4 address in dot-decimal notation (e.g., 192.168.1.1)
- IPv6 address in standard notation (RFC 5952 [2])
- telephone number in E.123 notation
- electronic mail address in E.123 notation
- Uniform Resource Identifier (RFC 3986 [3])
- geographic address

The Source field MUST be present -- to send a message anonymously, a sender MUST use one of the reserved entries of the different types. Reserved Entries for telephone numbers vary by region; for example, in North America they are 555-0100 to 555-0199. Reserved entries for IPv4 (RFC 5735 [4]), IPv6 (RFC 5156 [5]), and URIs (RFC 2606 [6]) may be found in their respective RFCs. The concept of a region defined by homogeneous communication characteristics has been put forward already in [7], so geographic addressing ambiguities may be resolved by community standards.

Because the message is sent to a specific geographical region, more leniency is available in source addressing, but requirements may be imposed by higher-level protocols.

We call this protocol the Asynchronous Dumb Visual Exchange of Raw Transmissions or ADVERT.

5.3. Transport Layer

Similar to the Network Layer, a Transport Layer protocol is able to omit several constructs that are used in existing Transport Layer protocols. Consider TCP -- sequence, acknowledgement, and many of the flags are discarded as there will be no SYN, SYN/ACK, or ACK handshake in a broadcast message. Likewise, fields such as Window Size and Urgent -- created primarily as a benefit to router manufacturers -- are unnecessary in this medium.

In fact, in the event of a plain text message, content SHOULD be embedded directly in the ADVERT Protocol without the need of a transport protocol. Consider the following packet:

```
          Content                          Source
+-----------------------------------------------------------+
| Lobster Dinner - only $14.99    500 Boardwalk, Pt Pleasant |
+-----------------------------------------------------------+
```

Figure 2: Example ADVERT Datagram

For UTF-encoded payloads, one SHOULD use the default UTF-encoding so the packet is human-readable. This will minimize accidental misinterpretation. This transmission structure lends itself most easily to human-parsable messages.

For messages intended to be responded to by a computer (for example, binary content), a Transport Layer protocol MUST be used, and an implementer SHOULD use UDP, as it is one of the more compact protocols available in this layer. An implementer SHOULD encode the UDP ports, length, and checksum in base-10 (leading zeros omitted) and the data in Base64 encoding. The Base64 encoding, combined with the UDP checksum, resolves ambiguities with trailing whitespace or non-printable characters.

The usage of UDP or other protocols that compute a checksum over source and destination addresses necessitates the use of either an IPv4 or IPv6 address as the Source in the ADVERT Protocol. The Destination address 255.255.255.255 MUST be used in the calculation of an IPv4-based checksum, as it has already been specified as a local hardware broadcast that must not be forwarded (RFC 919). For IPv6, the All Nodes link-local multicast destination FF02:0:0:0:0:0:0:1 MUST be used, defined in RFC 4291 [8].

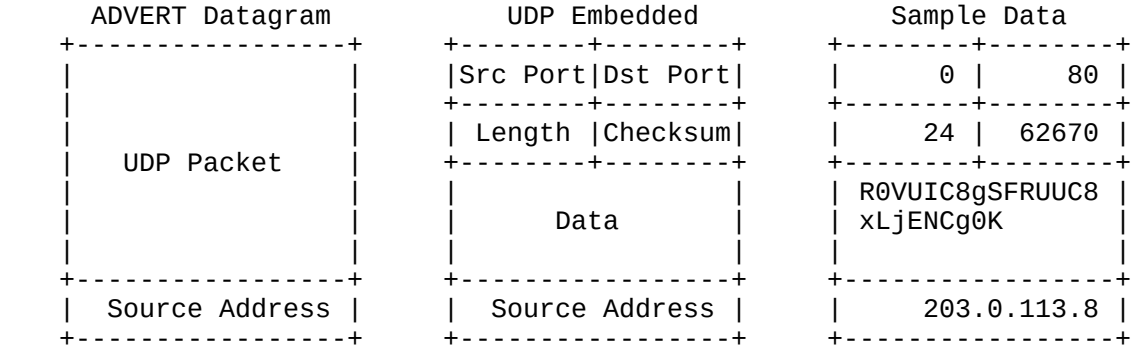

Figure 3: Example of Encapsulating Binary Data in an ADVERT Datagram

6. Reception

Upon receipt, the datagram should be optically scanned into an electronically transmittable form, similar to the methods used in RFC 1149 [9]. If present, any checksums SHOULD be computed and compared with supplied values. If the checksum does not match, the packet MUST be discarded.

Physical layers always have advantages and disadvantages depending on their condition, maintenance, prevalence, and economic factors; the atmosphere is no different. The protocols defined herein do not specify a TTL specifically because it is often out of their control, and dependent on the conditions present. The intrinsic TTL produces a curve of error rates where, after time, meaning cannot be deciphered from the datagram either because of a non-matching checksum or, in the absence of a checksum (such as the ADVERT protocol), because of an unintelligible transmission. If the Source field is sufficiently distinguishable, the recipient MAY contact the sender for message clarification. RFC 919 is in agreement in stating that broadcasts MUST NOT be assumed to have been reliably delivered.

Reconsidering Figure 3, a broadcast HTTP Request is sent, and recipients should return the request from each of their computer systems that are listening on the requisite port. It is important to remember the security implications of the systems' acceptance of data from unknown senders. It is the responsibility of each organization to utilize host-protection mechanisms and egress filtering to avoid exposing their systems to undue risk or exposing internal or NAT-ed devices.

Although it may be easy for an operator to silently discard the packet, it would be inappropriate for a network operator to unilaterally discard data, in the absence of policy. RFC 1087 [10] classifies an action that destroys the integrity of computer-based information as unethical and unacceptable; and the Code of Ethics of SAGE, USENIX, and LOPSA recognize the important of maintaining integrity, reliability, and availability.

7. Datagram Transmission

7.1. Chemical Approach to the Atmospheric Link Layer

Information is sent by transmitters producing a specialized form of smoke, most often by emitting a specialized oil onto the exhaust manifold. The oil, held in a pressurized container, is vaporized in a thick white smoke, producing readable display. The makeup of the smoke is often subject to patents, and any organization interested should consult with their attorneys. Further details on transmission

on the Physical Layer is beyond the scope of this RFC, but implementers MAY refer to references for help. It is by design that the broadcast mechanism does not result in incompatibilities if implementers choose different Physical Layer implementations.

7.2. Location

The datagram MUST be displayed in the atmosphere, at an altitude of 7000 to 17000 feet (2133 to 5181 meters). It SHOULD be written using a "skytyping" method, similar to dot-matrix printing (Figure 4). This method will provide better persistence of the datagram in the presence of air currents. Additionally, it provides the ability for parallelism by using additional avionic instruments.

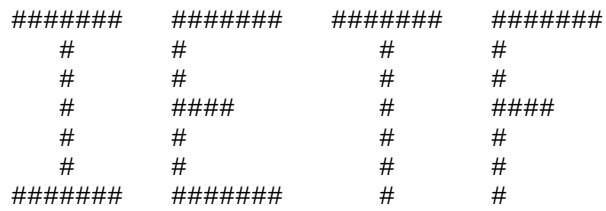

Figure 4: Skytyping Method in the Sky

The most efficient method for broadcasting a datagram on this link layer is the hire of specialized companies that perform this service on a regular basis. For a large organization interested in using this method frequently, it may be more cost-effective to develop one’s own methods.

7.3. Physical Layer Conditions

Transmission ability varies by atmospheric and regional conditions. Adverse conditions, such as an accumulation of moisture or ice crystals in the Physical Layer, may preclude transmission for a period of time. During these periods, it is suggested broadcasts be delayed, as higher-than-expected error rates may occur, and receivers may not be prepared to process the transmission immediately.

Additionally, solar radiation conditions affect transmission in a predictable, cyclic manner. Depending on latitude, the medium may be unusable for a lengthy period, during which alternate arrangements must be made.

Conditions may worsen before, during, or after a transmission, resulting in higher-than-expected transmission error rates. Regional operators should be familiar with their operating conditions and

consider the feasibility of implementing a casual or robust infrastructure on this transmission medium. Some locales lend themselves better to regular operation than others.

8. References

8.1. Normative References

[1] Mogul, J., "Broadcasting Internet Datagrams", STD 5, RFC 919, October 1984.

8.2. Informative References

[2] Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, August 2010.

[3] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[4] Cotton, M. and L. Vegoda, "Special Use IPv4 Addresses", BCP 153, RFC 5735, January 2010.

[5] Blanchet, M., "Special-Use IPv6 Addresses", RFC 5156, April 2008.

[6] Eastlake 3rd, D. and A. Panitz, "Reserved Top Level DNS Names", BCP 32, RFC 2606, June 1999.

[7] Hooke, A., "Interplanetary Internet", GSAW 2003, <http://sunset.usc.edu/gsaw/gsaw2003/s3/hooke.pdf>.

[8] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[9] Waitzman, D., "Standard for the transmission of IP datagrams on avian carriers", RFC 1149, April 1 1990.

[10] Defense Advanced Research Projects Agency and Internet Activities Board, "Ethics and the Internet", RFC 1087, January 1989.

Author's Address

Thomas Ritter
PO Box 541
Hoboken, NJ 07030
USA

EMail: tom@ritter.vg
URI: http://ritter.vg