

Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 7, 2020

K. O'Donoghue
IETF NOC Team
R. Hinden, Ed.
Check Point Software
November 4, 2019

IETF Meeting Network Requirements
draft-odonoghue-netrqmts-02

Abstract

The IETF Meeting Network has become integral to the success of any physical IETF meeting. Building such a network, which provides service to thousands of heavy users and their multitude of devices, spread throughout the event venue, with very little time for setup and testing is a challenge. This document provides a set of requirements, derived from hard won experience, as an aid to anyone involved in designing and deploying such future networks.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 7, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
1.1. Terminology	2
2. Requirements for Internet Connectivity	3
3. Meeting Facility Requirements	3
4. Internal Network Requirements	5
4.1. Requirements for Terminal Room or equivalent	5
4.2. Requirements for Wireless	6
4.3. Requirements for Services	6
4.4. Network Monitoring Requirements	7
5. Miscellaneous Requirements	7
6. Security Considerations	8
7. IANA Considerations	8
8. Acknowledgements	8
9. Revision History [RFC Editor: Please remove]	8
10. References	9
10.1. Normative References	9
10.2. URIs	9
Authors' Addresses	9

1. Introduction

The IETF Meeting Network has grown and evolved over time as has the IETF overall. In addition, the way that the IETF network is built and provisioned has also changed. It is time for the IETF community to consider the requirements of this infrastructure and its role in supporting the mission of the IETF. This document is meant to help frame that conversation. Additionally, this document may eventually be developed to be useful to others outside the IETF in specifying and building their own successful event networks.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Requirements for Internet Connectivity

- o A primary and backup link MUST be provided for redundancy. If technically feasible, these links SHOULD be aggregated or load balanced.
- o The primary and backup links MUST provide at least 1 Gbps bandwidth in both directions.

Recent events have peaked at roughly 850 Mbps and averaged in the 100-300 Mbps range. We expect peak bandwidth requirements to continue to grow at a roughly 40-60% compound annual growth rate.

- o IPv6 MUST be provided.
- o The transit provided in support of the IETF MUST be capable of providing access to the IPv4 and IPv6 default free zones without the imposition of content filtering (e.g., URL, Site, application, port, or DPI based filtering).
- o The primary and secondary links MUST support BGP peering.
- o The provider(s) MUST allow the IETF to advertise (from the IETF AS number) the IETF IPv4 and IPv6 address ranges.
- o The provider(s) MUST implement IRR (or better) route filtering.
- o The backup link SHOULD be supplied by a different Internet service provider from the primary link.
- o The primary and backup links SHOULD have physical and logical path diversity.
- o The provider(s) SHOULD carry and advertise full BGP tables.
- o The provider(s) SHOULD implement BGP communities, especially the ability to RTBH.

3. Meeting Facility Requirements

- o All locations for network gear, with the exception of wireless APs, MUST be secure.
- o If wireless will be used for an external link then access to the roof or installed location MUST be provided.

- o The meeting facility MUST have adequate ventilation to support the equipment rooms and the terminal room.
- o The meeting facility MUST have adequate power available to support the equipment required to support the network infrastructure and its users. This may include 110v/220v requirements in technical closets, roof locations, and various public and back-of-the-house areas.
- o The meeting facility MUST provide sufficient power in all meeting rooms to handle the projected load from users' laptops. The projected load is for simultaneous usage for 100% of the projected number of attendees in each meeting room and the number of laptop users and projecting 70 watts of power usage per laptop.

(?? do we want to provide actual power estimates?)

- o The meeting facility MUST provide the network installation team with access to key telecom spaces from one hour prior to the beginning of sessions to one hour after the end of sessions and 9am to 5pm daily during the setup period.

(?? are these the right timeframes)

- o The meeting facility SHOULD provide the network installation team with 24 hour access to key telecom spaces.
- o The meeting facility SHOULD have physical characteristics that support the deployment of additional wireless networks including techniques to limit interference where possible

(?? or something along those lines).

- o The meeting facility SHOULD have installed network cabling that can be used to deploy the network infrastructure.

(?? is this a should or must, are we past the days of running cable if we need to...)

- o The meeting facility The meeting facility SHOULD have Uninterruptible Power Supply (UPS) available to support key network infrastructure components, including at least the core routers, core switches, and hardware to maintain the external links.

4. Internal Network Requirements

- o Wired Ethernet connections (network drops) MUST be provided in all the locations used for meeting rooms to support audio and video distribution for the purposes of remote participation.
- o Wired network drops MUST be provided to the registration desk.

(?? need to confirm what the reg desk actually needs)
- o The network MUST NOT prohibit end-to-end and external connectivity for any traffic (no limiting firewalls or NATs).
- o The network SHOULD have separate VLANs for wired (primarily terminal room and audio) and wireless traffic.
- o The network SHOULD have mechanisms for detecting and silencing rogue servers (for example, DHCP, IPv6 RA's, etc.).

4.1. Requirements for Terminal Room or equivalent

- o A terminal room or quiet work space MUST be provided. This room MAY be a single room or distributed sites in reasonable proximity to the meeting rooms.
- o The IETF users MUST have access to the terminal room from ?? to ??.
- o Power strips MUST be provided in the terminal room.
- o The terminal room MUST provide at least one network connected enterprise class printer. These printers SHOULD have duplex capability.

(?? Is an enterprise class printer required? Have we been doing that?)
- o A color printer MAY be provided.
- o The terminal room SHOULD provide access to some number of wired Ethernet drops in addition to the standard wireless network.
- o There SHOULD be a manned help desk from ?? to ??. The help desk provides technical assistance to attendees, provides one potential interface to the trouble ticket system, and maintains the printers.

- o It is desirable that Power strips MAY be provided in common gathering areas.

4.2. Requirements for Wireless

- o The network design MUST anticipate simultaneous usage of 100% of the projected number of attendees in each meeting room. and the number of wireless network users (historical utilization in excess of 1000 simultaneous wireless users has been observed during a plenary session).
- o The network MUST provide Wi-Fi coverage in all meeting rooms (as identified by the Secretariat), common gathering spaces around the meeting rooms, the registration area, and the terminal room.
- o The network MUST provide at least one secure SSID and one open SSID.
- o The network SHOULD provide Wi-Fi coverage in additional common spaces in the meeting venue including the lobby, bar, restaurant, and most commonly used hallways of the primary meeting hotel(s).
- o The network MAY provide separate SSIDs for different specific requirements.
- o The network MAY provide additional secured wireless access.
- o There SHOULD be mechanisms for identifying and silencing rogue Wireless Access Points.

4.3. Requirements for Services

- o The network MUST provide redundant DHCPv4 servers.
- o The network MUST provide local redundant DNS servers.
- o Printers MUST support IPP and SHOULD support LPR and Windows printing.
- o The network MUST provide VMs for the Remote Participation Service.
- o The network SHOULD provide DHCPv6 service.
- o The network SHOULD provide NTP.

4.4. Network Monitoring Requirements

- o The network MUST provide sufficient monitoring to ensure adequate network availability and to detect faults before they impact the user experience.
- o The network MUST collect data for future use in scaling IETF meeting network requirements. Minimum required metrics include bandwidth utilization (average and peak) for each external connection and user density per AP and radio.
- o The network SHOULD provide some visibility into the state of the network for attendees (e.g. public graphs of network utilization, number of wireless associations, etc.).
- o The network provider SHOULD provide SNMP read-only access to the network devices to individuals as identified by the Secretariat for network management and planning purposes.

5. Miscellaneous Requirements

- o A document MUST be provided to attendees detailing on-site network configuration information, including wireless configuration details, services available (e.g., printing), instructions on how to report network issues (e.g. trouble ticket system interface instructions), etc. Initial versions of this information SHOULD be provided in advance of the meeting.
- o The network provider MUST NOT view the IETF network as an experimental facility at the risk of impacting the IETF attendee experience. (Do not experiment with his/her favorite pet technology.)
- o The network provider SHOULD maintain spares of critical network components on-site.
- o Attendees SHOULD be notified of power connector requirements well in advance of the meeting via the IETF meeting web page.
- o The network provider SHOULD have attended at least one prior IETF to observe the IETF network deployment and operation.
- o The network provider SHOULD supply the IETF network design to an IETF technical review team for comments.

6. Security Considerations

While security is clearly important to the design and delivery of the IETF meeting network. Draft -00 represents the information captured on the original 2009 version. Security requirements (and considerations) will be more clearly addressed in subsequent versions of this draft.

7. IANA Considerations

There are no IANA considerations for this document.

8. Acknowledgements

These requirements represent past and current NOC teams including hosts, volunteers, and network staff. All errors and misstatements are the responsibility of the current author.

Contributors to this draft include Warren Kumari, Clemens Schrimpe, and Alessandro Amirante.

Contributors noted in the original 2009 version of this document are (in no particular order): Jim Martin, Karen O'Donoghue, Chris Elliott, Joel Jaeggli, Lucy Lynch, Bill Jensen, Chris Liljenstoipe, Bill Fenner, Hans Kuhn.

Robert Hinden served as the document editor for this version of this document.

9. Revision History [RFC Editor: Please remove]

draft-odonoghue-netrqmts-02, 2019-Nov-4

- o First update since BOF at IETF 105
- o In each section reordered requirements in MUST to SHOULD order.
- o Restructured sections to be part of Internal Network Requirements.
- o Changes based on feedback on mailing list.
- o Added Robert Hinden as editor.
- o Editorial changes.

draft-odonoghue-netrqmts-01, 2019-July-8

This version incorporated initial comments received from the NOC Team. These were not fully discussed in advance of publication because of the looming deadline of the BOF at IETF 105.

draft-odonoghue-netrqmts-00, 2019-June-24

This version was an import of the text developed in 2009 and put on a website:

2009 IETF Network Requirements [1]

This was to ensure transparency by allowing the changes to be viewable in datatracker.

10. References

10.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

10.2. URIs

- [1] <https://www.ietf.org/how/meetings/admin/meeting-network-requirements/>

Authors' Addresses

Karen O'Donoghue
IETF NOC Team

Email: kodonog@pobox.com

Robert M. Hinden (editor)
Check Point Software
959 Skyway Road
San Carlos, CA 94070
USA

Email: bob.hinden@gmail.com