Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 26, 2019

K. O'Donoghue
IETF NOC Team
June 24, 2019

IETF Meeting Network Requirements
draft-odonoghue-netrqmts-00

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 December 26, 2019.

Table of Contents

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 build 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.

This document is currently being revised as part of an IETF community discussion on the network requirements for the IETF meeting network. Version -00 represents the requirements as articulated the last time these requirements was documented by the IETF NOC Team (https://www.ietf.org/how/meetings/admin/meeting-network-requirements/). The current draft plan is to update to a -01 that represents the requirements the IETF NOC Team currently builds to. Versions beyond that will represent input received from the community. A final version of this document may or may not be published depending on the desires of the IETF community and the potential usefulness of a document of this sort outside the scope of the IETF.

1.1. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

2. External 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 link MUST provide at least 45Mb bandwidth in both directions, and SHOULD have at least 100Mb bidirectionally. (Note: Historically, bandwidth utilization peaked at 80Mb and averaged 35Mb.

- o Recent events have peaked at 50 Mbs and averaged in the 25Mb range.) The backup link MUST have 10 Mb bandwidth in both directions and SHOULD have at least 45 Mb bandwidth in both directions.

- 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 IPv6 MUST be provided (possibly via a tunnel).

- 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 link MUST support BGP peering, and the backup link SHOULD support BGP peering.

- o Routing MAY be configured to allow the simultaneous usage of the bandwidth of both the primary and backup links.

- o Access to research networks, like those that are part of Internet 2, MAY be provided on one of the external links.

- o AS Numbers MAY be supplied by the network provider. If not, the network provider MUST use the AS Numbers provided by IETF.

- The network provider MUST provide at least a /19 of provider independent public IPv4 space or allow the IETF to advertise their own space.

- The network provider MUST provide at least a /32 of LIR public IPv6 space or allow the IETF to advertise their own space.

- If providing access space, the network provider MUST provide proper IP address delegation for DNS reverse lookups.

3. Meeting Facility

- The facility SHOULD have as much physical separation as possible in the meeting room area to improve the RF environment. In addition, the facility SHOULD avoid using airwalls and other partitions with low RF attenuation in the 2.4Mhz spectrum between meeting rooms.

- The facility SHOULD provide a RF environment in all meeting rooms (as identified by the Secretariat), common gathering spaces around the meeting rooms, the registration area, and the terminal room that has a reasonable noise floor in the 2.4Mhz spectrum.

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

- The meeting facility SHOULD provide the network installation team with 24 hour access to key telecom spaces. 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.

- All locations for network gear, with the exception of wireless APs, MUST be secure.

- If wireless will be used for an external link then access to the roof or installed location MUST be provided.

- The meeting facility MUST have adequate ventilation to support the equipment rooms and the terminal room.

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

- o The meeting facility MUST provide sufficient power in all meeting rooms to handle the projected load from users' laptops, using 100% congruency between the projected number of attendees in each meeting room and the number of laptop users and projecting 70 watts of power usage per laptop.

4. Internal Network

- o Wired Ethernet connections (network drops) MUST be provided in all the locations used for meeting room audio distribution for the purposes of audio recording and transmission.

- o Wired network drops MUST be provided to the registration desk.

- o The network SHOULD have separate VLANS for wired (primarily terminal room and audio) and wireless traffic.

- 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 mechanisms for detecting and silencing rogue servers (DHCP, IPv6 RA's, etc)

5. Terminal Room or equivalent

- o Terminal Room or equivalent A terminal room MUST be provided. This terminal room MAY be a single room or distributed sites in reasonable proximity to the meeting rooms.

- o The terminal room MUST provide Ethernet 10/100 connectivity with RJ-45 connectors (approximately 100-150 drops required). (note: this number should be revised based on terminal room usage statistics)

- o The terminal room SHOULD provide a small number of desktop or laptop computers for emergency use by attendees (minimum application requirements are web browsing, word processing, presentation production, and printing capability).

- o The terminal room SHOULD have 24 hour access. This access SHOULD include security, but it MAY not include a 24 hour staffed help desk.

- o The IETF users MUST have access to the terminal room from one hour prior to the beginning of sessions to one hour after the end of sessions.

- o The terminal room MUST provide at least two network connected enterprise class printers. These printers SHOULD have duplex capability.

- o A color printer MAY be provided.

- o The terminal room MUST have a manned help desk from one hour prior to the beginning of sessions to one hour after the end of sessions. The help desk provides technical assistance to attendees, provides one potential interface to the trouble ticket system (see next requirement), and maintains the printers.

- o The network supplier SHOULD provide a trouble ticket system to track attendee network issues. This trouble ticket system SHOULD be accessible to the help desk staff in addition to NOC staff.

- o Power strips MUST be provided in the terminal room.

- o Power strips MAY be provided in common gathering areas (desirable).

- o The terminal room MUST have physical security (guards) during operating hours.

6. Wireless

- o The network MUST provide 802.11b 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 SHOULD provide 802.11b coverage in additional common spaces in the meeting venue. The lobby, bar, restaurant, and most commonly used hallways of the primary meeting hotels, SHOULD also be provide 802.11b access.

- o The network SHOULD provide 802.11g in all the spaces identified above.

- o The network SHOULD provide 802.11a coverage in as many of the above identified spaces as possible focusing on the spaces with the highest user density first (e.g. plenary meeting room).

- o The network design MUST anticipate 100% congruency between 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).

- The network SHOULD provide separate SSIDs for 802.11b and 802.11a networks.

- The network MUST provide fully open (unsecured) wireless access.

- The network MAY provide additional secured (WEP, 802.11i, WPA) wireless access.

- There SHOULD be mechanisms for identifying and silencing rogue Wireless Access Points.

7. Services

- The network MUST provide redundant DHCPv4 servers.

- The network SHOULD provide DHCPv6 service.

- The network MUST provide local redundant DNS servers.

- The network SHOULD provide NTP.

- Printers MUST support IPP and SHOULD support LPR and Windows printing.

- The network MUST provide a SMTP server providing relay services for the IETF network.

- The network SHOULD provide a full on-site mirror of the RFC and I-D directories.

8. Network Monitoring

- The network MUST provide sufficient monitoring to ensure adequate network availability and to detect faults before they impact the user experience.

- 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.).

- 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 provider SHOULD provide SNMP read-only access to the network devices to individuals as identified by the Secretariat for network management and planning purposes.

9. Miscellaneous Requirements

- 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 both the IETF meeting web page and the IETF- announce mailing list.

- o A document MUST be provided to attendees detailing on-site network configuration information, including wireless configuration details, services available (e.g. printing, SMTP), 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 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.

10. 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.

11. IANA Considerations

There are no IANA considerations for this document.

12. Acknowledgements

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

Contributors noted in the original 2009 version of this document are (in no particular order):

- o Jim Martin
- o Karen O'Donoghue
- o Chris Elliott
- o Joel Jaeggli
- o Lucy Lynch
- o Bill "wej' Jensen
- o Chris Liljenstoipe
- o Bill Fenner
- o Hans Kuhn

Additional contributions including the current NOC Team will be added in subsequent versions of this draft.

Finally, the author is submitting this draft as an individual to help facilitate a conversation and as a long time volunteer member of the IETF NOC Team. This draft does not represent any official position of the Internet Society, her current employer.

13. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

Author's Address

Karen O'Donoghue
IETF NOC Team

Email: kodonog@pobox.com