Internet Engineering Task Force
Internet Draft
draft-pierce-ieprep-assured-service-req-02.txt
January 2004
Expires July 2004

Mike Pierce
Artel
Don Choi
DISA

Requirements for Assured Service Capabilities in Voice over IP
draft-pierce-ieprep-assured-service-req-02.txt

Status of this memo

Copyright

Abstract

Assured Service refers to the set of capabilities used to ensure that critical communications are established and remain connected. This memo describes the requirements for such capabilities in support of real-time communications for voice using specific networks such as those used by government agencies, but they could also be applied in commercial environments.

Table of Contents

1.   Introduction

Throughout many decades of evolution of the telephony network and its supporting protocols, there has been a need to provide preferential services and functionality to a limited subset of the users and calls within a network or domain in order to ensure completion of important calls that transit congested interconnections. Examples of this need have been in support of emergency traffic for natural disasters, network restoration traffic, and high priority traffic in a private networks. Provision of the required capabilities in the signaling protocols and within the switching systems has been defined in a number of national and international standards, most notably a service referred to as Multi-Level Precedence and Preemption (MLPP) as defined in an American National Standard [T1.619] in the US and in corresponding ITU-T Recommendations [I.255.3, Q.735.3, and Q.955.3]. In addition, a service called High Probability of Completion (HPC) was defined in the US [T1.631] and, most recently, two ITU-T Recommendations define the requirements for the International Emergency Preference Scheme

(IEPS) [E.106] and the International Preference Scheme for Multimedia Service in Support of Disaster Relief Operations [draft F.706].

Other drafts submitted to the IETF have addressed aspects of IEPS. Among these are the Framework for ETS for Telephony over IP [ETS].

MLPP was the solution for providing Assured Service capabilities within the circuit switched environment. It is essential that equivalent Assured Service capabilities are defined and implemented for the packet-based, connectionless environment of IP, and specifically SIP. Without these capabilities, SIP can not be used for those applications which require these capabilities.

This memo builds on these references and identifies the specific requirements for Assured Service capabilities for Voice applications in support of these specific types of environments. Although this memo covers only Voice, there will be similar requirements for "Assured Service" capabilities for all other forms of communication. The term "Assured Service" is used to refer to the required capabilities, rather than the previous term of "MLPP" or the related but different terms of IEPS or ETS, since the envisioned set of capabilities and protocols to achieve them are not expected to be exactly the same as those other services. For example, IEPS/ETS may not have a requirement for preemption at any point in the SIP session, whereas Assured Service may at both the session endpoint and in networks between endpoints.

Although these requirements are derived from previous government applications, many of the same requirements and capabilities may be applied for non-government networks, for example, in support of commercial network restoration efforts. A presentation in the TEWG during the August 2001 meeting demonstrated real-life situations from the past in which total network failures required extensive efforts, presumably including communication via other unaffected networks, to bring the affected network back on line. If one considered a situation in which the very network which had failed was needed to carry the network management traffic required to get it back on line, it would be hard to imagine how it could ever be brought back up in the face of overwhelming customer attempts. Capabilities would be required to give priority to the network management traffic, even to the extent of blocking all non-emergency traffic for a period of time.

1.1. Changes

Note: This section will be deleted before progressing as an RFC.

This document has evolved through 2 different working groups:

SIPPING and IEPREP. This draft was originally submitted under SIPPING with 2 revisions. It is now in the IEPREP WG in order to ensure that the Assured Service requirements are considered along with those of the related IEPS discussions

(SIPPING) -00 Original draft

(SIPPING) -01 Indicated informative material which would not be a part of final. Moved some to Annex.

(SIPPING) -02 Removed material to draft-pierce-sipping-pref-treat-examples-00 and draft-pierce-sipping-assured-service-arch-00. Added requirement to maintain records of use of service.

(IEPREP) -00

. Updated references.
. Added additional requirements related to preferential treatment in 4.3.
. Added requirement in 4.8 for accounting records.
. Added requirement in 4.9 that preferential treatment must be applied to call control signaling as well as to voice packets.
. Added requirement in 4.10 for interworking between Assured Service and other priority schemes (e.g., IEPS)

(IEPREP) -01

- Updated references
- Moved informative material to Annex
- Clarified requirement statements

(IEPREP) -02

- clarified some text
- made individual requirements into bulleted, named items instead of freeform text
- moved additional informational material to a separate draft

2. Background

In the circuit switched environment, specific circuits or channels are used for each call. These are typically 64 kbps channels which were normally part of a Time Division Multiplexed (TDM) transmission structure. These transmission channels are almost always interconnected and switched by Time Division Switching technology (often referred to as "TDM switching").

More recent developments use packet/cell based transport instead of dedicated 64 kbps channels, often coupled with packet/cell-based switching, however, the effect is the same. There is still a dedicated transport capacity assigned for each call.

Assured Service in the circuit switched environment may be provided by one or more of the following techniques.

. Giving priority to return of dial tone (IEPS - note)

. Marking of signaling messages for better handling, for example, being last to be dropped in case of congestion in the signaling network (HPC)

. Extra routing possibilities for higher priority calls (IEPS - note)

- Queuing for network resources (HPC)

. Exemption from restrictive management controls such as hard-to-reach codes and code gapping (IEPS - note)

. Reservation of specific facilities (trunks) for higher priority traffic (IEPS - note)

. Higher priority calls may preempt existing lower priority calls, causing the network to release the lower priority call to free up resources for immediate reuse by the higher priority call (MLPP)

(Note: Capabilities included within IEPS [E.106] are listed here for reference only but are not dealt with further in this document.)

Identification of traffic authorized to use one or more of these techniques may be via the following or similar methods:

. Calls placed from physical lines or devices authorized for signaling a higher priority for a call

. Calls placed to specific telephone numbers or blocks of numbers

. Entry of a special ID code and PIN from any telephone device to identify that this call should receive special service.

. Use of a "smartcard"

3. High Level Requirements

While the existing requirements and capabilities have been developed with the circuit switched environment in mind, many are directly applicable to the packet environment and specifically the Voice over IP application being defined using SIP. Some of the capabilities need to be adapted or modified for application in the packet mode environment. In addition, there will likely be new techniques which can be defined specifically for the SIP case.

At a high level, the Assured Service requirements can be stated as the need to ensure that mission critical voice-mode calls get set up and remain connected.

As a result of this, calls designated as being at a lower precedence level are presumed to be less important and may be adversely affected by various techniques used to provide the preferential treatment to the important, mission-critical calls. For example, the lower precedence calls may temporarily experience reduced quality as their packets are discarded.

This memo does not address issues related to incorrect assignment of the authority to use precedence levels or the incorrect use of levels, for example, if the user can not or does not specify a high enough precedence level for the nature of the call.

(While this memo focuses on Voice over IP, there should be a consideration of the impact/solutions for other media flows which carry mission critical communication, for example, file transfers, video, and instant messaging. Most of the functional requirements can be equally applied to these other media.)

4. Functional Requirements

While the functional requirements for Assured Service detailed here are specifically those needed to support the US government requirements for the Defense Switched Network (DSN), it is believed that at least a subset of those requirements are applicable to other government networks as well as some commercial (non-government) networks. This memo concentrates on those portions mentioned in Section 2 which are derived from the requirements for MLPP as defined in the American National Standard [T1.619].

The basic requirements are defined as follows;

4.1. Precedence Level Marking

Each call or session within an Assured Service network is labeled with a precedence level as determined by the calling party at the beginning of the call. If not chosen by the caller, the default is to the lowest precedence level. The called party does not have any control over the precedence level for a call or session.

To meet this general functional requirement, the following specific requirements apply:

Prec-1 It MUST be possible to assign each user the highest precedence level they are entitled to use.

Prec-2 It MUST be possible for the originator of a call to select and signal one of the multiple precedence levels for the call, with the call defaulting to the lowest level if none is specified. The precedence of each call is independent, that is, it is selected for each call.

Note: One current network for which this is intended uses five levels, but other numbers of levels are possible. In no case is it necessary to support more than 15 levels.

Prec-3 It MUST be possible to carry this call associated precedence level unchanged though the IP network as a part of the Call Control Signaling (for example, in SIP).

Prec-4 It MUST be possible to deliver the originally signaled precedence level to the called party.

4.2. Authentication/Authorization

Not all users are allowed to signal higher precedence levels. Therefore, a means is necessary to determine and allow only the authorized users the ability to signal these higher precedence levels. The following specific requirements apply:

A&A-1 It MUST be possible to verify that the calling party is authorized to use the Assured Service and the requested precedence level value if higher than the lowest.

A&A-2 It MUST be possible to take the appropriate action if the calling party attempts to use a level which is higher than authorized. The preferred action is to reject the call, and send an indication of the reason to the caller.

4.3. Preferential Treatments

Since it is expected that congestion may occur in various parts of a network, it is required that one or more preferential treatments can be applied to any call or session which is signaled with a higher precedence level relative to already existing calls or sessions if that call would cause congestion. This is required to manage the effects of congestion, for example, delay, delay variation, and loss, at key points. The actual measures applied depend on the situation, but support for the following are required:

4.3.1. Call/Session Treatment

Pref-1 It MUST be possible to block setup of a new call if that call would cause congestion. This is called Call Admission Control (CAC).

Pref-2 It MUST be possible to apply different limits for CAC for various call precedences, that is, in some cases, a higher precedence call may be allowed to be established while a lower precedence would not.

Pref-3 It MUST be possible for an endpoint to release an existing (lower precedence) session in favor of completing a new session signaled to it (at a higher precedence).

Pref-4 It MUST be possible for a network node to release an existing network resource reservation in favor of a higher precedence session. This might involve releasing one or more reservations in the process of providing enough bandwidth for the new packet flow.

Pref-5 Preferential treatment SHOULD NOT be provided through any scheme of dedicated or pre-reserved bandwidth or resources.

Pref-6 In those cases in which such dedication or reservation of bandwidth or resources is used, when such dedicated or pre-reserved bandwidth or resources have been consumed by the high precedence traffic, further traffic of that same high precedence MUST NOT be provided worse treatment than any of the lower precedence levels.

4.3.2. Packet Transfer Treatment

Pref-7 It MUST be possible at any point of congestion to determine which packets require preferential treatment over other packets, including for voice media packets.

Pref-8 It MUST be known by the device experiencing congestion what to do with two or more competing packets.

Pref-9 It MUST be possible for a network node to discard packets for lower precedence calls in favor of those for higher precedence calls.

Pref-10 Media packets MUST NOT starve all potential bandwidth of a node interface, thus not allowing signaling packets through that same interface. (Note that this requirement is not unique to Assured Service.)

4.3.3. Procedural Requirements

Pref-10 It MUST be possible to detect various congestion conditions which might require preferential treatments to be applied.

Pref-11 Preferential treatment measures used to manage congestion MUST be automatic and MUST NOT have to be manually "turned on" in reaction to a congestion event of any kind.

Pref-12 The application of preferential treatment MUST not require a significant delay to activate (such that it is noticeable to the party originating a precedence call).

Possible methods of providing Preferential Treatment using the provisions of this memo, as well as other existing IETF protocols, are described in [Pierce1].

4.4. Diversion if Not Answered

In situations is which the called party is busy and can not be preempted or in which the called party does not answer, it is required to provide a diversion service to a predetermined address for any call signaled with a precedence level above the lowest. The following apply:

Div-1 If a precedence call (one higher than the lowest level) is blocked by the called party being busy with a call of equal or higher precedence, the call MUST be diverted to a predetermined alternate party.

Div-2 If a precedence call is not answered within a designated time, the call MUST be diverted to a predetermined alternate party.

While the actual requirement previously was for a single "diverted-to" address for an entire "switch", this is not feasible in the IP case, so the specification of the "diverted-to" address is assumed to be per called user. In general, it is expected that this diversion capability will operate similar to a normal "Call Forwarding on No Answer" service.

4.5. Notifications

It is required that a user who is currently on a call/session and is preempted either at the remote end or in between be notified of this event. Generally a distinct tone is provided, after which the call/session is released.

Noti-1 All preempted parties MUST be provided with a distinct notification informing them that their call has been preempted.

Specific notifications are required to inform the calling party of reasons for a precedence call not being successful. They are the following:

Noti-2 When a user attempts to use a precedence level to which they are not authorized, the caller MUST be notified of this fact. The notification MUST NOT provide an indication of what level is authorized.

Noti-3 When a precedence call can not be established due to the called party being busy at an equal or higher precedence with no alternate party diversion possible or due to no preemptable resources in the network, the caller MUST be notified of this fact. The caller MUST NOT be notified what precedence level would be necessary to successfully complete the call.

4.6. Acknowledge by Preempted Party

When a user is involved in a call/session and that call/session is preempted in favor of establishing a higher precedence call/session with that same user, the user is required to actively accept this new call before the media is connected. This is no different from normal calls.

Ack-1 When an existing call has been preempted for delivery of a higher precedence call to the same party, the party MUST acknowledge the preemption before the new call is connected. That is, there MUST be a positive acknowledgement before any audio information is transferred in either direction.

4.7. Protection of Signaling/Routing Information from Disclosure

Although protection is not actually an integral part of the Assured Service functionality, it is specifically identified here since this capability is generally required in those networks which are assumed to be the primary users of Assured Service.

Prot-1 Sensitive information MUST NOT be made available to non-secure portions of the network or to any non-secure network through which the traffic passes.

Prot-2 Sensitive information MUST NOT be accessible by users connected to the network.

Prot-3 Precedence information regarding each call (as well as the other information such as calling/called party identity) SHOULD be protected from disclosure.

This non-disclosure requirement especially applies to information which is used to control link state routing protocols based on knowledge of the current traffic load at each precedence level on each route or through each router.

4.8. Accounting

Proper administration of the Assured Service capability requires that use of the service can be reviewed after the fact for potential abuse.

Acct-1 It MUST be possible for the appropriate records to be kept of calls made, including the calling and called parties' identities, time of the call, duration, and the precedence level used. This is similar to the requirements for Call Detail Recording (CDR) for billing purposes for other services in a commercial environment.

4.9. Call Control Signaling Precedence

Since it competes for the same transport resources as the voice packets, it is essential that preferential treatments can be applied to the call control signaling. Specifically the following apply:

CC-1 The call control signaling MUST NOT adversely affect the voice (e.g., by introducing excessive packet delay variation due to extremely long messages).

CC-2 The voice traffic MUST NOT significantly delay important call control signaling (e.g., by preventing release messages from getting through).

4.10. Interworking

Although Assured Service will likely be the only priority scheme within many network using it, it still needs to interwork with other schemes.

Int-1 Assured Service calls MUST interwork with other priority schemes which are being provided within the same network, such as the one defined for [ETS]. This includes the following two cases:

a. both types of traffic may exist in a single network, for example, an IEPS call may be originated from within a network which also supports "Assured Service" calls. Procedures to determine the relative priority and the resulting preferential treatment are required.

b. a network which provides "Assured Service" needs to support interworking of calls to and from a network which provides another scheme such as IEPS as well as another network which provides "Assured Service". Mapping between the precedence levels of the two networks must be supported.

5. Security Considerations

5.1. Authentication/authorization of User Access

There is a need within SIP to authenticate/authorize all access to capabilities, since virtually any function could be misused, resulting in harm to the network or to other users. Because Assured

Service is intended to provide an authorized user with better service than other users, including the potential of actually preempting resources, it is even more important to authenticate/authorize the user's access to the Assured Service capabilities. However, the requirement already exists for all cases, not just Assured Service, therefore the solution is not unique to Assured Service.

5.2. Security of Signaling Information

The need to protect signaling information from disclosure is independent from the provision of Assured Service. Many networks have long been built on the premise that such information needs to be protected. Bulk encryption of signaling links (as well as the user data channels) between secure switches provided much of this protection. In addition, the Signal Transfer Points of the SS#7 network could be physically secured against unauthorized access. It should be noted that commercial networks have recognized the need for the same level of protection previously only applied to various government networks.

In the IP environment, the signaling packets traverse many routers and could be accessed by unauthorized persons at any one of them. While the contents of the individual signaling messages could be hidden by encryption of the request and response for end-to-end protection of information, the IP header must be visible to intermediate routers. It is preferable to not require decryption/ encryption at each router. The approach has been to encrypt the contents of the IP packets (the signaling message) but not the IP headers which are needed by the routers. However, the IP headers themselves may contain sensitive information such as precedence level and ways to identify the called party, or least the location of the called party.

5.3. Security of Routing Data

In IP today, there is no Routing Data to secure. When enhancements are made to provide for route selection, especially to route around congestion, procedures must be developed to prevent unauthorized access to that data. It is presumed that procedures will also be required to prevent unauthorized modifications.

5.4. Security of User Data

While there may typically be a greater need to protect the user data (voice packets) of a call which utilizes priority, since such a call may often be more sensitive than calls for which no priority is specified, this requirement is not unique to the Assured Service, and therefore no specific requirements are given here. The same requirements exist for non-Assured Service traffic.

6. IANA Considerations

There is no IANA involvement in support of Assured Service beyond what is described for the Resource Priority Header [Resource].

7. References

[T1.523] ANSI T1.523-2001, "Telecommunications Glossary".

[T1.619] ANSI T1.619-1992 (R1999) and ANSI T1.619a-1994 (R1999), "Multi-Level Precedence and Preemption (MLPP) Service, ISDN Supplementary Service Description".

[T1.631] ANSI T1.631-1993 (R1999), "Telecommunications - Signalling System No. 7 (SS7) - High Probability of Completion (HPC) Network Capability".

[E.106] ITU-T Recommendation E.106 (2003), "International Emergency Preference Scheme for Telecommunications for Disaster Relief Operations(IEPS)".

[F.706] ITU-T Recommendation F.706 (draft), "International Preference Scheme for Multimedia Service in Support of Disaster Relief Operations and Mitigation".

[I.255.3] ITU-T Recommendation I.255.3 (1990), "Multilevel precedence and preemption service (MLPP)".

[Q.735.3] ITU-T Recommendation Q.735.3 (1993), "Description for community of interest supplementary services using SS No. 7 - Multilevel precedence and preemption (MLPP)".

[Q.955.3] ITU-T Recommendation Q.955.3 (1993), "Description for community of interest supplementary services using DSS1 - Multilevel precedence and preemption (MLPP)".

[RFC3261] "SIP: Session Initiation Protocol", J. Rosenberg, et al, June 2002.

[ETS] draft-ietf-ieprep-framework-06, "Framework for Supporting ETS in IP Telephony", Ken Carlberg, et al, Oct 2003.

[Pierce1] draft-pierce-ieprep-pref-treat-examples-02, "Examples for Provision of Preferential Treatment in Voice over IP", Mike Pierce, et al, January 2004.

[Resource] draft-ietf-sip-resource-priority-01, "SIP Communications Resource Priority Header", Henning Schulzrinne and James Polk, July

2003.

8. Acknowledgements

The authors would like to thank James Polk and Fred Baker for the many suggestions made to improve this document throughout its development.

9. Authors' Addresses

Michael Pierce
Artel
1893 Preston White Drive
Reston, VA 20191
Phone: +1 410.817.4795
Email: pierce1m@ncr.disa.mil

Don Choi
DISA
5600 Columbia Pike
Falls Church, VA 22041-2717
Phone: +1 703.681.2312
Email: choid@ncr.disa.mil

Full Copyright Statement