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

Mike Pierce
Artel
Don Choi
DISA

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

Status of this memo

Copyright

Abstract

Assured Service refers to the set of capabilities used to ensure that mission critical communications are setup and remain connected. This memo describes the architecture required to meet the requirements detailed in [Pierce1].

Table of Contents

0. History

This draft was originally submitted under SIPPING. This revision is being submitted under IEPREP to be included in the discussions for related services such as IEPS.

(SIPPING) -00: Original

(IEPREP) -00: Added Access Router to architecture required to support Assured Service.

-01 Updated references

-02 Updated references and minor editorial changes.

1. Introduction

The requirements for Assured Service are given in [Pierce1]. Many other drafts and RFCs have addressed the assumed architecture for the provision of SIP-based services. A lot of consideration has been given to continued reliance on the pure peer-to-peer model on which the Internet (and especially HTTP) has been based vs. migration to centralized control models in which dedicated proxies perform specific functions for the control of telephony services. This would include, possibly, full knowledge of the state of each call.

While there is an wide-spread desire expressed in various IETF discussions to maintain (or return to) the pure peer-to-peer architecture, there has been increasing admissions in various drafts that centralized control or intelligent "middleboxes" are required in many cases. Some examples are:

1. RFC 3261 defines the notion of a "Call Stateful proxy", which "retains state for a dialog from the initiating INVITE to the

terminating BYE request", i.e., for the duration of a call. However, no use of this state has been included in the current version of SIP [RFC3261].

2. Draft-ietf-sipping-cc-framework-02 included the concept of a "central control" signaling model.

3. The abstract for draft-ietf-sipping-service-examples-05 recognizes that "some [services] require the assistance of a SIP Proxy", and it states that the flows shown assume "a network of proxies, registrars, PSTN gateways, and other SIP servers that have a pre-established trust relationship with each other... User agents wishing to use the services in this network are required to authenticate themselves with an edge proxy...".

4. RFC 3325 for identity and privacy is based fully on use of a network of trusted SIP servers. It states that "these mechanisms provide no means by which end users can securely share identity information end-to-end without a trusted service provider."

2. Architectures

Various discussions and memos have identified two potential network architectures for the provision of SIP services. They are briefly:

2.1. End-to-end Architecture

All service provision is between and under control of the calling and called party, referred to as "User Agent Client (UAC)" and "User Agent Server (UAS)", respectively. This terminology of "client" and "server" are based on the HTTP model from which this model is derived and have no real significance to this model. Either end can initiate a transaction. There is no device in-between which provides service support, only routers for packets. Other required devices (address translation, etc.) which the calling user must access are simply additional UAS's.

There is no "Service Provider" for the voice service, only a provider of the packet switched infrastructure.

2.2. Service Provider Network Architecture

A Service Provider maintains and controls network elements which play an active role in the provision of services to end users. These network elements may be referred to as back-to-back user agents (B2BUA), proxies, servers, middleboxes, or intermediaries but they all have the common characteristic of being provided by a trusted Service Provider and they provide an important logical function between the end users. These elements terminate SIP messages,

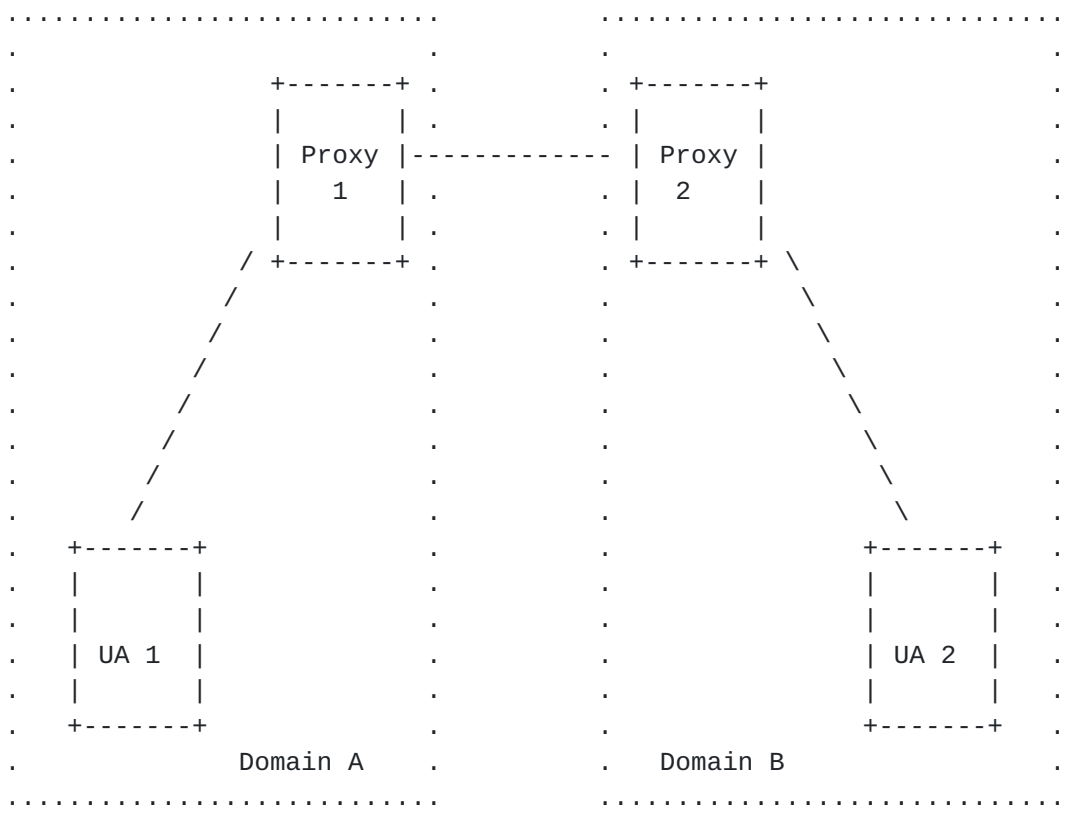
perform service control, and send new or modified SIP messages to other network elements or to the other user. The result is that no

SIP message goes directly from one UA to the other (unless specifically authorized by the control element).

The "Service Provider" may be the same company or entity which provides part or all of the packet switched infrastructure.

3. Required Architecture

In order to provide the security and feature control required for Assured Service as defined in [Pierce1], it is necessary to utilize the Service Provider Network Architecture in which proxies are used to support call origination and termination for each user involved in the service. The architecture is the "trapezoid" described in SIP [RFC3261] as follows (figure actually copied from RFC 3263):



Interfaces:

(1) Originating UA 1 to Proxy 1: Authentication and all SIP messages to/from UA 1
(2) Proxy 1 to Proxy 2 (and to other devices such as policy servers): SIP messages and policy actions
(3) Proxy 2 to terminating UA 2: Authentication and all SIP messages to/from U 2
(4) Originating UA 1 to terminating UA 2: Voice packets, no

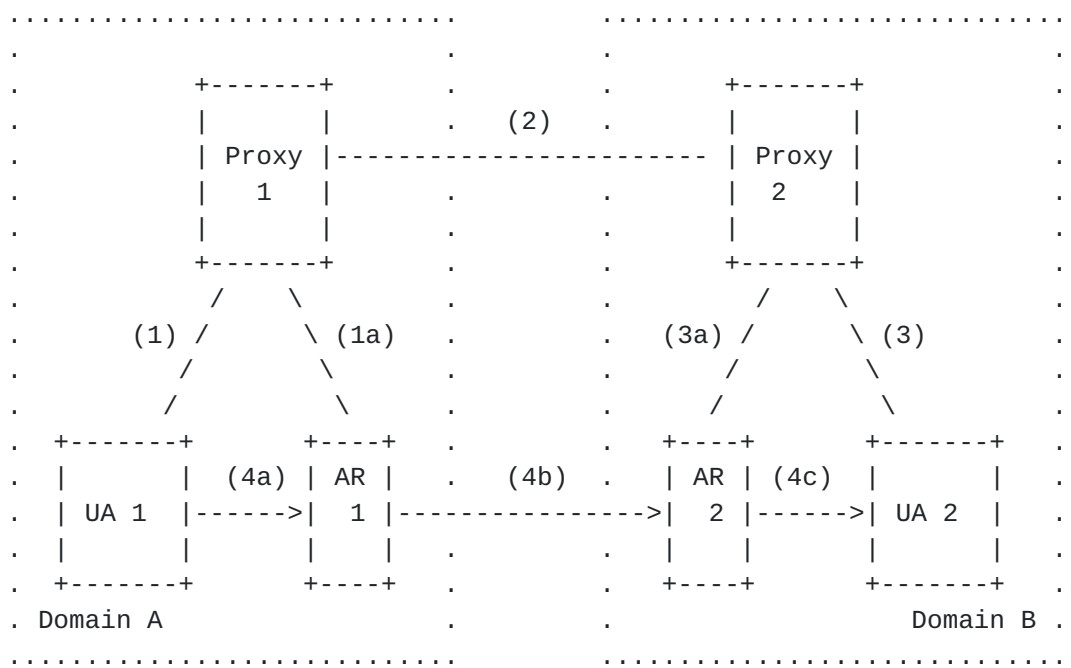
signaling messages

However, the above architecture requires the addition of another

component to provide control of the user's data packets (voice) in the Assured Service case. This is important since the packets themselves need to be marked for preferential treatment, including the ability to get "priority" over the packet transfer of another user.

There must be an access router, generally at the boundary between the local network and the core network. This may be between the Ethernet LAN and the IP "cloud" or it may be between the locally controlled IP network and the global IP network. In any case, its function is to regulate the transport of priority marked packets into the core.

The following figure depicts this architecture:



Interfaces:

(1) Originating UA 1 to Proxy 1: Authentication and all SIP messages to/from UA 1
(1a and 3a) Proxy to AR: instructions to allow voice packet transport
(2) Proxy 1 to Proxy 2 (and to other devices such as policy servers): SIP messages and policy actions
(3) Proxy 2 to terminating UA 2: Authentication and all SIP messages to/from U 2
(4a) Originating UA 1 to AR 1: attempted voice packets
(4b) AR 1 to AR 2: authorized voice packets
(4c) AR 2 to UA 2: authorized voice packets

4. Required Procedures

4.1. Authentication

Each UA which might use the Assured Service capability must authenticate with a designated proxy before any service activation is attempted. Normally, this would be at the time the device is powered on, connected to the network, or is initialized, or it might be done at pre-determined time intervals. Whether or not this authentication requires a user interaction (human entry of a password, retina scan, etc.) is not important and depends on the application. Such an authentication may be very time consuming, with password verification and policy data-base look-ups. After this authentication, this proxy must handle all session establishments, both to and from this UA.

This authentication function may be performed when the user attempts the first session setup, for example, when an individual is allowed to use a common device by first "logging on" with their identity and password. In fact, this is still an "authentication" function performed before the session setup is attempted. However, in this case, it must be understood that there may be an additional delay due to the authentication process before a call can be placed.

This authentication process is not unique to the provision of the Assured Service capability. It is also required for many other services which are to be provided by the service provider's proxy based on pre-established authorizations.

4.2. Function of Proxy

Besides the processing of the authentication, each proxy is responsible for a number of functions important to the provision of Assured Service (as well as other services) and the handling of interactions, where required, between different services. This includes (for Assured Service):

. maintaining state of all existing sessions, including their priority, which exist on all UAs under its control (both proxies).

. maintaining knowledge of other services being used by the UA which might need to be taken into consideration when applying the Assured Service capabilities (both proxies).

. verifying that the originating UA is allowed to establish the session at the precedence level requested (originating proxy).

. establish permission at the access router for it to handle the precedence marked packets from the UA (both proxies).

- performing the timing function to control the diversion service (terminating proxy).

- deciding when to preempt the end user and sending the appropriate preempt messages to the other party (both proxies).

- maintaining records of the use of the service, whether for accounting or auditing purposes (both proxies).

4.3. Function of the Access Router

The access router, under control of the proxy, decides which packets are to be transported between networks or domains. If authorization has not been granted for the transport of a specific packet flow at the precedence level indicated in the packets, the access router must discard the packets.

Additionally, there may be cases in which a currently transported packet stream must be stopped. Since the Assured Service may not be able to rely on the UA to stop the flow, it may be necessary for the access router, again under control of the proxy, to stop transporting a particular flow.

4.4. Session Control

Session establishment and release should follow the same message sequence as defined in SIP and its extensions for non-Assured Service calls. There should not be any additional messages for an Assured Service call. The only additional requirements are the inclusion of:

- the priority level as defined in [Resource] in the INVITE

- security related information in every message which might consist of an authentication header (AH) using cryptographic techniques to allow the receiving end (user or proxy) to validate the authenticity of the message before acting on it. (This requirement is not unique to Assured Service, but is also required to secure other capabilities.)

5. Security Considerations

This memo mostly deals with the architecture required to support the necessary security. While it does not attempt to define the actual security mechanisms used for authentication and authorization, it establishes the service architecture required as a basis for security.

6. References

[RFC3261] RFC 3261, "SIP: Session Initiation Protocol", J. Rosenberg, et al, June 2002.

[RFC3313] RFC 3313, "Private SIP Extensions for Media Authorization", W. Marshall, May 2002.

[RFC3323] RFC 3323 "A Privacy Mechanism for the Session Initiation Protocol (SIP)", J. Peterson, November 2002.

[RFC3325] RFC 3325, "SIP extensions for Network-asserted Caller Identity and Privacy within Trusted Networks", C. Jennings, et al, February 2002.

[Pierce1] draft-pierce-ieprep-assured-service-req-02, "Requirements for Assured Service Capabilities in Voice over IP", Jan 2004.

[Resource] draft-ietf-sip-resource-priority-00, "SIP Communications Resource Priority Header", Henning Schulzrinne and James Polk, June 2003.

7. 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

document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other