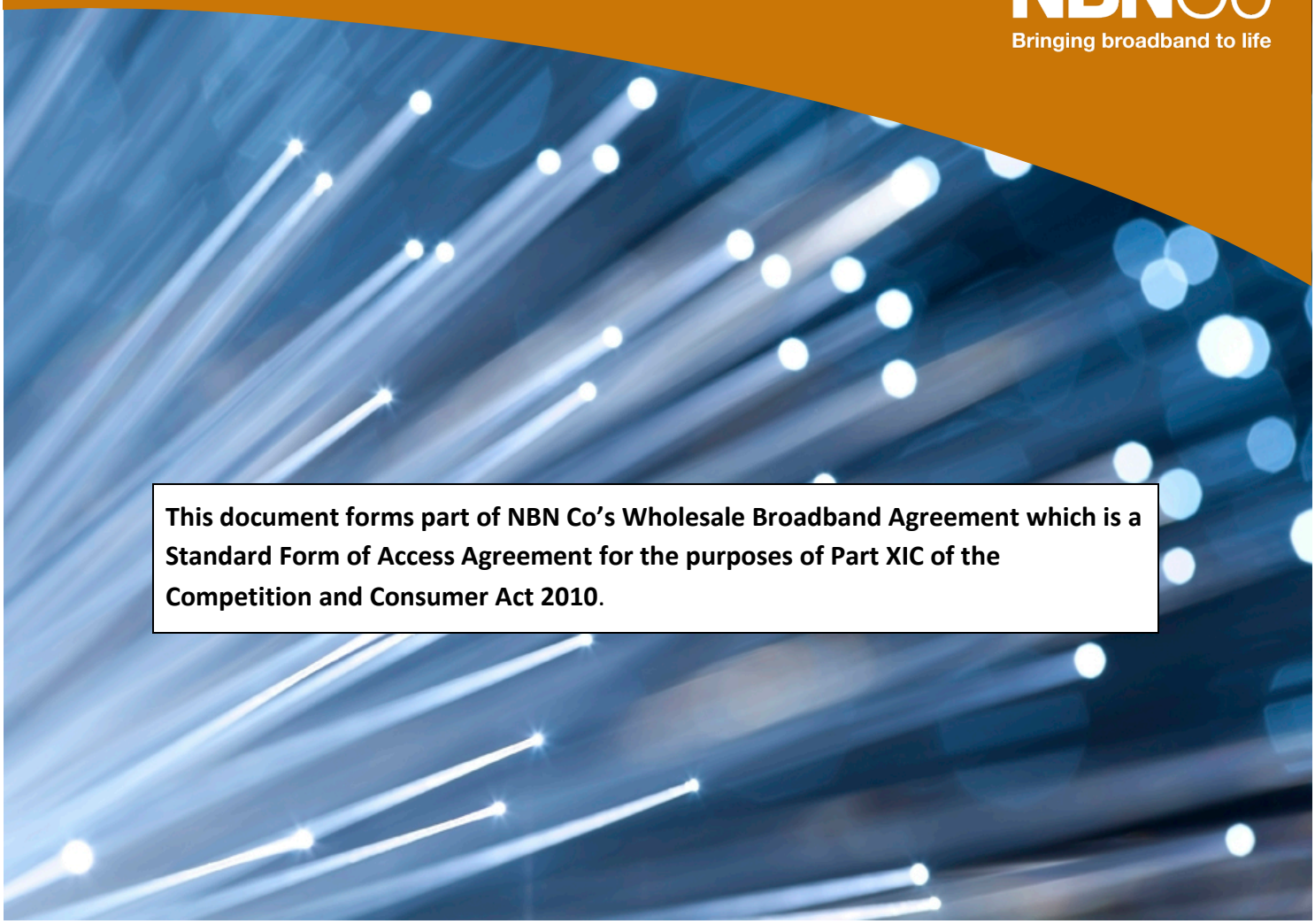
NBN Co Fibre Access Service

UNI-V FUNCTIONAL SPECIFICATION – FIFTH RELEASE

28 AUGUST 2013

NBNCo
Bringing broadband to life



This document forms part of NBN Co's Wholesale Broadband Agreement which is a Standard Form of Access Agreement for the purposes of Part XIC of the Competition and Consumer Act 2010.

NBN Co Limited

NBN Co Fibre Access Service – UNI-V Functional Specification – Fifth Release

28/08/2013

Version: 5.0

Disclaimer

From time to time Customer may be able to access undocumented features and functionality of the UNI-V. Customer must not use features or functionality not explicitly described by the UNI-V specification. Such features or functionality may not operate as expected, will not be supported by NBN Co, and may change without any notice to Customer. Customer must not rely on those features and functionality continuing to be available unless expressly supported by NBN Co as described in a formal specification.

Environment

NBN Co asks that you consider the environment before printing this document.

Table of Contents

Summary of Figures

Summary of Tables

1. NFAS Telephony Service overview

The NBN Co Fibre Access Service (**NFAS**) has been designed to support the provision of telephony services by access seeker to End Users using the UNI-V. The UNI-V has been designed to support carrier grade PSTN equivalent telephony services for the support of complex services by access seeker to End Users, such as security/medical alarms, fax, EFT, TTY and other voice band data services. The features and functions of the UNI-V have been developed with industry, in the context of current Australian Customer Premises Equipment (**CPE**) standards.
This approach has been adopted to seek to maximize the extent to which current CPE will interoperate with the UNI-V. However, there may be existing CPE (such as certain legacy equipment) which may not interoperate with the UNI-V. NBN Co is continuing to work with industry on these aspects.

If access seeker wishes to provide telephony services (including IP connectivity, signalling and media traffic) to its End Users using the NFAS and UNI-V, access seeker will need to acquire and utilise the following product components of the NFAS:

- Network to Network Interface (**NNI**)
- N:1 Traffic Class 1 Connectivity Virtual Circuit (**CVC**)
- Access Virtual Circuit (**AVC**)
- UNI-V on the Network Termination Device (**NTD**)

Where utilised in accordance with the terms of the Wholesale Broadband Agreement, the UNI-V will terminate telephony signalling protocols and functions.

NBN Co has designed traffic handling mechanisms that are tailored toward specific applications. Within the NBN Co Network, Traffic Class 1 is designed to accommodate the deterministic performance required for real-time, conversational applications including telephony services. Capacity within this traffic class is available to access seeker via the dedicated AVC that terminates on the UNI-V and on the corresponding CVC, facilitating a high quality telephony service experience for End Users.

When using the UNI-V, access seeker utilises the Analogue Telephony Adaptor (**ATA**) port that is in-built into the NTD, with integrated Session Initiated Protocol (**SIP**) capabilities for legacy telephony applications. A range of configuration options are available to enable access seeker to migrate an existing telephony service, and deliver a PSTN-similar telephony service to the UNI-V port of an NTD installed in respect of the End User's Premises with minimal impact to in-building wiring or equipment installed at the end user's premises.

Alternatively Access seeker may provide telephony services to End Users using the UNI-D on the NTD. This requires access seeker to provide its own ATA. The scope of this document does not pertain to this service construct. Please refer to the Product Technical Specification for the NBN Co Ethernet Bitstream Service.

1.1. Feature support and Roadmap Overview

In this release of the NBN Co Fibre Access Service UNI-V, there are changes to capability and characteristics of the UNI-V from previous releases of the UNI-V. These changes may affect how access seeker delivers an IP telephony service to its End Users. Service configuration of the UNI-V is based on the Broadband Forum TR-069 method which utilises access seeker's own Auto Configuration Server (**ACS**) for the configuration of the UNI-V.

This release of the UNI-V supports the following features and capabilities:

- Quality of Service (**QoS**) support for TC_1 traffic class (As described in the Product Technical Specification for the NBN Co Ethernet Bitstream Service)
- connection to a dedicated AVC per UNI-V
- SIP signalling with RTP stream
- Two UNI-Vs per NFAS NTD
- Discrete SIP UA per UNI-V
- A single RJ11C interface per each UNI-V 2-wire interface
- G.711 A law companding codec
- 20ms packetisation rate
- TN12 complex impedance
- Configurable Dial Plan with support for emergency numbers (000/106)
- Voice features
    - Softswitch features such as call forwarding (Busy, No answer and Unconditional)
    - Call hold
    - Call Waiting
    - Suspend Call Waiting
    - Hotline immediate
    - Distinctive ring cadences
- Voice band data using G.711A clear channel
    - Fax up to 9.6 kilobits per second
    - Modem up to 14.4 kilobits per second
    - TTY support
    - Tone detection for the suppression of echo cancellation and Comfort Noise Generation
- Calling Line Identification Presentation (**CLIP**)
- Calling Line Identification Restriction (**CLIR**)
- Calling Number Display
- Message Wait Indication (**MWI**)
    - Visual indicator
    - Audible Stutter Tone
- Ringer Equivalence Number (**REN**) of up to 3 per UNI-V
- DTMF Tones passed as either in-band or RFC2833 out of band
- Line voltage break of less than one minute during reboots and upgrades
- Metallic Line Test

- Battery backup as described in the Product Description for the NFAS
- Dial Plan up to 1024 characters
- Additional speed tiers for CVC TC_1 Data Transfer Rates
- Support for the TR-069 CPE WAN Management Protocol (CWMP) to allow an access seeker's ACS to configure the SIP UAs.
- TR-104 standard as the data model format for telephony parameter configuration.
- RTCP

1.2. Scope

This document applies in respect of this release of the UNI-V features and capabilities only.

This document does not apply to the UNI-V deployed in the Tasmania Tri-Area Service zone.

This document describes the interface specification for the NFAS telephony services at the NNI and UNI-V. It does not apply in respect of NBN Co services other than the NFAS.

Section 2 describes the UNI-V solution, Layer 2 connectivity at the NNI and bandwidth requirements.
Section 3 describes the UNI-V network connectivity including DHCP negotiation.
Section 4 describes UNI-V software maintenance.
Sections 5**,** 6 **and** 7 describe the TR-069 implementation characteristics and operation, covering detailed use case scenarios and supported diagnostic parameters.
Sections 8 **and** 9 describe the call features supported, the SIP client configuration and the expected SIP flows between the UNI-V and access seeker's softswitch.
Section 10 describes TR-098 and TR-104 parameter configuration.

This document is intended to provide a technical guide on the functional specification of the UNI-V to access seeker.

Except for explicit statements to the contrary, this technical specification does not exclude the need to satisfy the requirements of other Australian technical standards and/or other NBN Co technical requirements.

1.3. Purpose

The purpose of this document is to specify the capabilities and characteristics of the UNI-V and NNI interfaces that access seekers interface with to deliver their IP telephony service to their end users.

This document discusses the design principles for each of the interfaces:

- the UNI-V in regards to the logical interface characteristics and the SIP client design including telephony features supported and SIP configuration requirements to allow telephony connectivity between access seekers and their end-users; and
- The NNI in regards to layer 2, layer 3 and bandwidth requirements.
- The TR-069 solution supported on the NTD in relation to the UNI-V, which describes the UNI-V CPE WAN Management Protocol (**CWMP**) client and its support for TR-069 data model extensions.

1.4. Intended Audience

This document is intended to be used by access seekers that wish to utilise the UNI-V for the provision of voice or voice band data telephony services to an end user.

1.5. Relevant Documents

This document is to be read subject to the latest versions of:

- the NFAS Product Description;
- the NBN Co Ethernet Bitstream Service Product Technical Specification; and
- the UNI-V Electrical Specification.

If there is any inconsistency between this document and any of the above documents, then that inconsistency will be resolved by giving precedence to documents in the order listed, with this document and the UNI-V Electrical Specification to be given equal precedence.

1.6. Definitions

The table in section 11 sets out the meaning of certain words, acronyms and abbreviations that are used throughout this document.

Any capitalised words used throughout this document that are not defined in section 11 have the ordinary meaning commonly accepted in the industry.

References to an access seeker will be read as a reference to the Customer for the purposes of the Wholesale Broadband Agreement.

2. Solution Overview

Delivery of telephony services to the UNI-V utilises an IPoE service model where DHCP is used for direct allocation of an IP address in respect of a UNI-V to the NTD installed at an End User Premises.

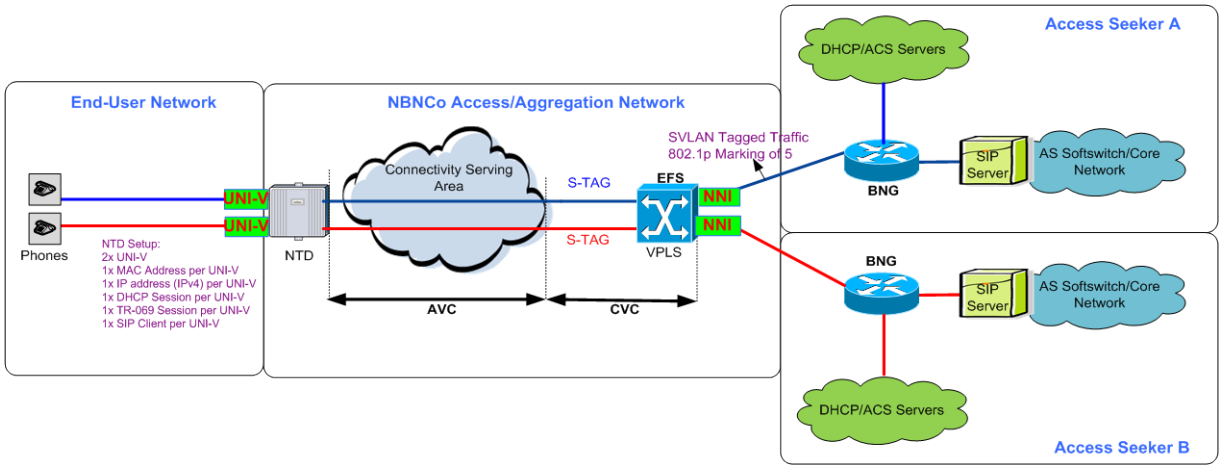


Figure 1 - End-to-End Telephony Service Overview

The UNI-V will provide the following capabilities per UNI-V:

- Unique MAC address
- IP address
- SIP User Agent (**UA**)
- Dedicated DHCP session
- Dedicated TR-069 session to communicate to access seeker's ACS
- TR-104 object model for voice service provisioning

2.1. UNI-V Contextual Overview

Each UNI-V is located on an NTD as described in the Product Description for the NFAS and the Product Technical Specification for the NBN Co Ethernet Bitstream Service. The following characteristics of the NTD are relevant to understanding the functional operation of each UNI-V:

- NTDs have two integrated 2-wire interfaces visible to the End User and both of these UNI-Vs are orderable by access seekers. Both UNI-V's on the same NTD may be ordered and operated by either a single access seeker, or by two access seekers simultaneously. Where two access seekers simultaneously offer telephony services on the same NTD, each access seeker will be able to access and operate their allocated UNI-V only.

- Each UNI-V may only be used by access seeker for the purpose of transmitting voice and data traffic in the voice band.

- Each UNI-V supports residential POTS telephones.

- Each UNI-V supports 0.3-3.4kHz audio, with an R-Value in the range 80-93, when used with the G.711 codec.

2.2. UNI-V and PSTN Equivalence

The NFAS with a UNI-V Product Component utilising the G.711 A-Law codec (the same codec that is used for the Australian PSTN) is designed to facilitate access seeker using the NFAS to provide an End User with a service which the End User can use to replace a PSTN service in most common scenarios.

A PSTN service may carry telephony services such as dialup modems, fax machines, set-top boxes (with PSTN authentication), TTY and security/medical alarms. The End User may be unaware that some of these devices rely on an existing PSTN connection. NBN Co has not tested all devices that rely on a PSTN service. NBN Co implements the recommended settings in Table 1.

Parameter	G.711 A-Law codec
Voice Quality on local call (G.107 usable range 50-100)	80-93
PSTN-similar Voice Quality	Supported
Support fax/data calls	Supported

Table 1 - Recommendations for G.711

Codec	Packetisation	Average media bandwidth (kbps)	PSTN-equivalent
G.711A-Law	20msec	101	Yes

Table 2 - G.711 overview

For incoming calls, the UNI-V will use the packetisation interval offered in the INVITE for both the transmit and receive packetisation interval.

2.3. Disability Support

(a) The UNI-V supports the operation of an in-band TTY device.

(b) The UNI-V supports the use of a telephone in parallel with TTY for VCO/HCO applications.

2.4. Network-Network Interface (NNI)

The NNI is a physical interface (and associated ports) between the NBN Co Fibre Network and access seekers' network at the POI, as described in the Product Description for the NFAS and the Product Technical Specification for the NBN Co Ethernet Bitstream Service.

2.4.1. Layer 2 Addressing Model

The NNI design principles relevant to use of the UNI-V are as follows:

- NBN Co implements the N:1 forwarding model for telephony services delivered via the UNI-V.
- At the NNI, End User traffic is presented and received as single-tagged 802.1Q (and 802.1ad) compliant frames. The S-TAG represents the CVC, and the individual AVC services are represented by the unique MAC address of the UNI-V.
- At the NNI, **access seeker must set the Service VLAN 802.1P PCP=5 for both signalling and media traffic** (in accordance with further details specified in the NBN Co Ethernet Bitstream Service Product Technical Specification) before ingress to the NBN Co Network at the NNI. Mismatched or incorrectly set values will cause traffic to be discarded by the NBN Co Network. Please note that the signalling traffic includes protocols such as ARP, DHCP, DNS, ICMP and HTTP.
- At the NNI, all traffic will be mapped to PCP=5 before being forwarded to access seeker's network.
- All service frames egressing the NBN Co Network at the NNI (i.e. from the NBN Co Network to access seeker's network through the NNI at the POI) must traverse an IP device before being injected back into the NBN Co Network. This is necessary to avoid UNI-V MAC addresses from appearing as source addresses on traffic ingress to the NBN Co Network at the NNI. This operating restriction must be observed by access seeker even if service frames are being switched between VLANs or forwarded via other service provider networks.
- The Service VLAN ID value at the NNI will be configurable upon request by access seeker, at the time the CVC is created.
- Upstream DHCP traffic on an AVC will be marked with an AVC service identifier allocated by NBN Co. This will be inserted in the DHCPv4 request (Option 82 Circuit ID) messages from the NBN Co Network OLT and can be used by access seeker to authenticate the End User and/or automatically instantiate End User forwarding instances on its edge or BNG devices. The Circuit ID (option 82) set by NBN Co will provide the AVC identifier (format "AVCnnnnnnnnnnn" where n = digit).
- A unicast N:1 CVC and a unicast 1:1 CVC can coexist on the same NNI interface by using different S-TAG VID values to differentiate them.
- Access seeker must ensure the layer 3 MTU size is 1500 bytes to safely carry the largest SIP signalling and TR-069 packets.
- It is possible for an access seeker to order more than one CVC in a Connectivity Serving Area (**CSA**). Where this is the case, specific AVCs within that CSA must be carried in the CVC they were originally provisioned against.
- It is access seeker's responsibility to provide Call Admission Control (**CAC**) on the CVC, so that the number of simultaneous calls does not exceed the capacity of the CVC, otherwise latency, jitter and frame loss will increase, impairing voice and data communications.

- Simultaneous frames from different calls may exceed the capacity of the CVC (e.g. as a result of traffic bursts) and hence affect media latency, jitter and frame loss impairing voice and data communications. An Access Seeker can implement QoS policies within their network to minimise the effects of traffic bursts.

- TR-069 and SIP traffic are allocated Traffic Class 1 (TC-1) Data Transfer Rates. Access seeker should therefore consider TR-069 and SIP traffic (generating bursts) while voice calls are in progress on an AVC.

2.4.2. Bandwidth Distribution

The following are the traffic definitions, guidelines and principles of the bandwidth distribution intended to be provided by the NBN Co Network:

- TC-1 (802.1P PCP=5) is a high priority traffic class designed for applications that require low latency, jitter and frame delay. Recommended usage is voice and Voice Band Data (**VBD**).

- Each UNI-V is provisioned in conjunction with a minimum AVC bandwidth of 150Kbps TC-1 (CIR) Data Transfer Rate. For example, if access seeker supports 500 telephony end users, it will need to order 500 UNI-V and AVC Product Components. ICMP echo (and any concurrent signalling e.g. SIP, RTP, DHCP, ARP, DNS and TR-069), when used as a connectivity test, will be subject to the traffic policing of the TC-1 traffic class service.

- The CVC TC-1 bandwidth (that aggregates the AVC TC-1 traffic) can be purchased in the increments set out in the WBA Product Catalogue.

- On the downstream from the access seeker network towards the NBN Co network, it is recommended that access seekers implement Call Admission Control (CAC) function. This will determine the amount of bandwidth available, weighed against the amount of bandwidth currently in use, to be able to control the number of simultaneous telephony sessions that can be carried in the available bandwidth. Ongoing capacity management of the orderable components (such as AVC, CVC and NNI) is the responsibility of access seeker.

- The NBN Co Network will police and drop any access seeker traffic that exceeds ordered CVC and AVC bandwidth.

2.4.3. Security

At the application level, telephony services offered are transported using transparent OSI layer 2 services and as such, with respect to the UNI-V and the NNI, there are no specific access seeker security constraints.

The solution design prevents communication directly between NTDs. All IP traffic from a UNI-V will need to traverse access seeker's NNI and layer 3 devices before reaching another UNI-V.

The UNI-V will initiate a TR-069 configuration request to the access seeker ACS with the HTTP password being hashed using the MD5 algorithm. However, when access seeker's ACS initiates a TR-069 session with a UNI-V, the UNI-V will authenticate the ACS with a HTTP connection request password.
The UNI-V does not support SSL or TLS in its CWMP client.

3. UNI-V Network Configuration

The UNI-V provides an analogue 2-wire POTS interface intended to provide a similar performance to the PSTN (when paired with gateways of similar quality, selecting suitable codecs and echo canceller modes, and allocated sufficient bandwidth).

3.1. IP Addressing

At the network level, the UNI-V supports the IP addressing parameters set out in the table below.

Network parameter	Description
IP address of UNI-V	Used for all SIP signalling, bearer traffic, and management functions. Each UNI-V has a unique IP address which is configured using DHCP
IP subnet mask	Configured using DHCP
Default IP router	Configured using DHCP
DNS IP address	Optional DNS server IP address. This is obtained using DHCP option 6.
ACS IP address	For ACS dynamic configuration of the UNI-V. Obtained using DHCP option 43. The IP address of the ACS can be provided as an IP address or a fully qualified domain name in the DHCP offer.
IP address of Registrar	Configured in the Registrar Server parameter in SIP Provisioning data. Either an IP address or a domain name may be configured.
IP address of SIP server	This is the address of the softswitch and is configured in the outbound proxy parameter. Either an IP address or a domain name may be configured along with a port number
IP Proxy Server	This is the domain name or IP address of the SIP proxy server. If the outbound proxy parameter is not configured, the UNI-V will use this parameter to forward SIP signalling traffic to.

Table 3 - UNI-V IP addressing parameters

Addresses in the range 192.168.1.0/24 and 192.168.2.0/24 are reserved for UNI-V internal use and must not be used as part of a telephony service using the UNI-V.

3.2. DHCP Options supported

DHCP option	Function
1	IP subnet mask
3	Default IP router
6	DNS server address
43	Vendor specific information
51	IP address lease time of the UNI-V
53	DHCP message type
54	DHCP server identifier
55	Parameter request list
60	Vendor Class Identifier (contains string “dslforum.org” for ACS server address query)
82	Circuit ID (will be added to DHCP request by the NBN Co Network)

Table 4 - DHCP Options supported on the UNI-V

The DHCP server should normally extend the existing IP lease, as a change in IP address may disrupt calls or TR-069 sessions in progress. Access seeker should consider the effect of DHCP lease times. NBN Co recommends that DHCP leases should be approximately a day in length.

3.2.1. DHCP Option 43

In the DHCP discovery message initiated by the UNI-V at boot up, the DHCP discovery message will include a DHCP Option 60 - Vendor Class Identifier value. The value for DHCP Option 60 consists of a string "dslforum.org". This can be used by access seeker's DHCP server to identify that the UNI-V supports the TR-069 based solution. The DHCP server will then send the DHCP Offer with the **Vendor Specific Information** (DHCP option 43) containing CWMP information.

This option allows access seeker's DHCP servers to send the vendor specific parameters to the UNI-V, encoded in the form "option_code/value_length/value". CWMP specifies two parameters:

- Option code 1 for ACS URL which will consist of the ACS FQDN (or IP) and port
- Option code 2 for the ProvisioningCode.
- Option code 254 for provisioning the logical ID of the UNI-V. The contents of this option code will be used as the value of the parameter "**InternetGatewayDevice.DeviceInfo.SerialNumber"** in TR-069 messages generated by the UNI-V.

When the UNI-V receives the URL it can start the standard CWMP connection and operations with the given ACS.

The DHCP Option 43 payload has a maximum length of 255 bytes (characters) due to being an 8-bit length field. This will be distributed between option code 1 (ACS URL), option code 2 (ProvisioningCode), option code 254 (logical ID) and a 2-byte sub-option headers for each option code.

3.2.1.1. Option Code 254 Logical ID

When values in Option 43, option code 254 are present, these details will be used instead of the default TR-069 "**SerialNumber"** parameter for TR-069 transactions. This is intended to allow the access seeker to create their own ID population or reuse the AVC-ID as it suits them. When Option 43, option code 254 data is not present, the UNI-V will fall back to using the default TR-069 "**SerialNumber**" parameter derived from the NTD's own serial number.

An example of the NTD serial number is ALCL12345678.

An example of the default TR-069 serial number is ALCL1234567801 (i.e. "NTD serial number" appended with "01").

An example of the AVC-ID is AVC000000012345.

Option code 254 is a sub-option in DHCP Option 43 that is configured by access seeker's DHCP server. The value provided by this option code should be unique to each End User service and, when present, will be used by the UNI-V to populate the "**SerialNumber**" field under "**InternetGatewayDevice.DeviceInfo".**

This value, in addition to the "DeviceInfo" parameters (i.e. Manufacturer, OUI and ProductClass), can be used by access seeker's ACS to uniquely identify the UNI-V and allow for pre-provisioning of the ACS prior to the UNI-V initial connectivity.

NBN Co recommends that access seeker configures DHCP Option 43 option code 254 with the same value as the AVC ID, as it is unique for each End User service
The following paragraphs set out characteristics of option code 254 and its limitations:

1. To avoid conflict with potential future option codes that may be added to TR-069, option code 254 is implemented after URL option code 1 and ProvisioningCode option code 2.

2. If access seeker decides to implement option code 254, it is then essential that the DHCP server include the same valid option code 254 at every DHCP negotiation (e.g. DHCP Offer, ACK etc.) with the UNI-V, otherwise a "0 BOOTSTRAP" event will occur (see paragraph 7 below). DHCPNAKs generally do not trigger a change in the Serial Number in use or trigger a "0 BOOTSTRAP" event, but following DHCP OFFERs or ACKs may do so.

3. The maximum length supported for option code 254 is 63 characters/bytes.

4. The value provided to the UNI-V in option code 254 should only use characters from the character set: {'0'..'9'}, {'a'..'z'}, {'A'..'Z'} to be configured. Presence of characters outside this set will cause the value to be treated as invalid by the UNI-V, resulting in a default TR-069 SerialNumber being used.

5. Option code 254 is considered invalid in the following failure scenarios:

    a. If the DHCP server configures the UNI-V with option code 254 that has a 0 length (i.e. empty).

    b. If the DHCP server configures the UNI-V with option code 254 greater than 63 characters/bytes.

    c. If the DHCP server configures the UNI-V with option code 254 that contains characters outside the allowed character set above.

6. When the UNI-V is first created/activated the UNI-V will proceed with an initial DHCP lease acquisition and, if present, use the value conveyed in DHCP Option 43, option code 254 for the TR-069 SerialNumber. If option code 254 is not present or invalid the UNI-V will use the **default TR-069 serial number** when communicating with the ACS.

7. In subsequent DHCP negotiations (e.g. during DHCP lease renewal), the following alternatives are available:

    a. If a valid option code 254 value is received:

        i. If the value received is the same as the serial number currently being used, the UNI-V will take no action.

        ii. If the value received is different to the serial number currently being used, the UNI-V will trigger a “0 BOOTSTRAP” message to the ACS that includes the new option code 254 value.

    b. If an invalid option code 254 value is received:

        i. If the current serial number being used matches the default TR-069 serial number, the UNI-V will take no action.

        ii. If the current serial number being used does not match the default TR-069 serial number, the UNI-V will trigger a “0 BOOTSTRAP” message to the ACS that includes the default TR-069 serial number.

    c. If option code 254 is not present:

        i. If the current serial number being used matches the default TR-069 serial number, the UNI-V will take no action.

        ii. If the current serial number being used does not match the default TR-069 serial number, the UNI-V will trigger a “0 BOOTSTRAP” message to the ACS that includes the default TR-069 serial number.

8. The UNI-V, whether using the default TR-069 serial number or one received in option code 254, stores the serial number state such that an UNI-V does not unnecessarily trigger a “0 BOOTSTRAP” event when the NTD is power cycled.

9. If access seeker is disconnecting a UNI-V so that another access seeker can place an order for that UNI-V, or if access seeker is connecting to the UNI-V after another access seeker has disconnected from that UNI-V (i.e. a churn event), the UNI-V configurations will be deleted, and NBN Co will re-provision the UNI-V with new default configuration details as described in this UNI-V Functional Specification. In this case, the UNI-V state and configuration will be cleared and the UNI-V will behave as in the “first created/activated” case in paragraph 6 above.

3.2.2. DHCP Option 43 Server Configuration

NBN Co recommends that access seeker configure its **DHCP Server with option 43** using the **option vendor-encapsulated-options** option shown in the "dhcpd" configuration script example below. There are three fields in this option as follows:

- Option_code
- Value_length
- Value

```
subnet 192.168.0.0 netmask 255.255.255.0 {
    option routers 10.1.1.1;
    range 10.1.1.100 10.1.1.105;
    append dhcp-parameter-request-list 43;
    option vendor-encapsulated-options 01:26:68:74:74:70:3a:2f:2f:31:32:2e:30:2e:30:2e:34:32:3a:38:31:38:31:2f:64:70:73:2d:64:69:67:65:73:74:2f:54:52:30:36:39:02:05:41:42:43:44:45:FE:0F:41:56:43:31:32:33:34:35:36:37:38:39:31:32:33
```

As an example, if the ACS URL to be used is http://12.0.0.42:8181/dps-digest/TR069, the option will contain 0×01 (CWMP option for ACS URL), 0×26 (hexadecimal of decimal 38 = length of the URL) then the other 38 bytes will form the URL value.

01:26:68:74:74:70:3a:2f:2f:31:32:2e:30:2e:30:2e:34:32:3a:38:31:38:31:2f:64:70:73:2d:64:69:67:65:73:74:2f:54:52:30:36:39:

Option code 2, the ProvisioningCode, is included in the **option vendor-encapsulated-options** option (representing the credentials ABCDE). This specifies the credentials used by the UNI-V to authenticate for the first time with access seeker's ACS. The hexadecimal value for the option 2 is **02:05:41:42:43:44:45**.

Option code 254 will include the logical ID of the UNI-V (e.g. AVC123456789123) and will also be included in the **option vendor-encapsulated-options.** This specifies the SerialNumber value in the TR-069 messages initiated by the UNI-V. The hexadecimal value for option code 254 is **FE:0F:41:56:43:31:32:33:34:35:36:37:38:39:31:32:33**

Note that DHCP Option 43 on the DHCP server must have the option codes configured in exact sequential order. That is, access seeker must configure DHCP Option 43 with option code 1 (URL) followed by option code 2 (ProvisioningCode) followed by option code 254 (Logical ID). The UNI-V will only accept the option codes if they are received in this specific order.

3.2.3. Duplicate IP Addresses

Where both UNI-Vs of a single NTD are in use by different access seekers, there is a possibility that both UNI-V's will be configured with the same IP address.

When a UNI-V is configured with a duplicate IP address, the UNI-V subsequently configured with the same IP address will issue a DHCP DECLINE as per RFC-2131 and will attempt to acquire a new address from the DHCP server. The UNI-V will repeat this process until a new non-conflicting address has been assigned. The UNI-V cannot be configured by the access seeker ACS whilst this conflict exists.
It is therefore important that the access seeker DHCP server automatically handles the DHCP DECLINE and issues a new address that is not conflicting with the adjacent UNI-V in order to restore the UNI-V service.

This condition will be cleared when the UNI-V sends a DHCP Discovery and will stay cleared if the UNI-V is configured with a non conflicting IP address.

4. UNI-V Maintenance

In cases of NBN Co maintenance, such as NTD firmware upgrade or NTD replacement, access seeker should consider the following:

1) At the time of the maintenance activity: Access seeker should have the DHCP server configured with DHCP option 43 to configure the NTDs with the access seeker ACS URL and ProvisioningCode and Option Code 254 (logical ID).
2) In the case of a major upgrade or device replacement it may be necessary to reprovision UNI-V services via ACS. In these cases a CWMP BOOTSTRAP 0 event will be generated by the NTD to the ACS URL served via DHCP. The ACS must be available at the time of upgrade to reconfigure UNI-V telephony services. This is similar to new service creation or factory reset.
3) In other cases, such as minor NTD software update, the NTD will issue a BOOT event once powered up and connected to the access seeker's ACS.
4) The upgraded UNI-V will continue to use the originally allocated associated AVC-ID.

If an Emergency Call (as defined by access seeker's dial plan as described in section 8.2.1.14) is found to be in progress immediately before the migration begins, the NTD firmware upgrade will be postponed. Firmware will only be upgraded once the emergency call is terminated. Other call types may be terminated by migration activities. Access seeker has responsibility for communicating potential service interruptions to its End Users.

5. TR-069 Overview

UNI-V management in accordance with TR-069 is performed through the communication between a UNI-V and the Auto-Configuration Server (ACS). The ACS task is to manage subscribed UNI-Vs in a flexible and systematic way. An ACS in general is a server machine running a manager application.

TR-069 will provide access seeker with a one common platform to manage all UNI-Vs which NBN Co is supplying to access seeker. It commonly uses HTTP as the transport for communication between each UNI-V and the ACS.

UNI-V support for TR-069 provides access seeker's ACS the following functions:

- Auto Configuration and dynamic service provisioning; the protocol allows the ACS to perform auto-configuration and to provision the UNI-V with services based on a variety of criteria. The provisioning of a UNI-V might be done when the UNI-V initiates a connection to the access seeker network or when the UNI-V initiates re-provisioning at any subsequent time. The identification mechanism allows provisioning based on specific requirements of a UNI-V; group criteria such as vendor, model, software version, or other criteria.
- Diagnostic parameters supported by TR-069 (as set out in section 7) allow access seeker's ACS to retrieve status information from the UNI-V in order to help resolve connectivity or service issues.

In TR-069, the UNI-V acts as the HTTP client and the ACS acts as the HTTP server. A SOAP request from an ACS to the UNI-V is sent over an HTTP response, while the UNI-V's SOAP response to an ACS request is sent over a subsequent HTTP Post.

The table below sets out the TR-069 CWMP protocol stack including a description of each layer.

Layer	Description
UNI-V /ACS Management Application	The application uses the CPE WAN Management Protocol on the UNI-V and ACS, respectively. The application is locally defined and not specified as part of the CPE WAN Management Protocol.
RPC Methods	The specific Remote Procedure Call methods that are defined by the CWMP. Remote Procedure Calls are encoded in SOAP. All messages exchanged between the UNI-V and ACS are RPCs. RPCs are methods that allow one program on a host machine to use the services of another program in a remote machine. The calling program sends a message and data to the remote program, which is executed, and results are passed back to the calling program.
SOAP	A standard XML-based syntax used to encode remote procedure calls. SOAP 1.1 is used to configure the UNI-V.
HTTP	HTTP 1.1 as specified in RFC2616.
SSL/TLS	The standard Internet transport layer security protocols. The UNI-V does not support SSL/TLS for configuration using the TR-069 protocol.
TCP/IP	Standard TCP/IP.

Table 5 - Brief description of protocol layers

5.1. TR-098 and TR-104 Data Model Extensions

The CWMP client on each UNI-V supports those CWMP parameters that are defined in the following two technical reports and set out in sections 10.1 and 10.2:

1) TR-098: Internet Gateway Device data model for TR-069; this defines the parameters related to IP network configuration on the UNI-V. The UNI-V supports the subset of parameters in the following objects which are described in sections 10.1 and 10.2:
    a. DeviceInfo; Providing information about the UNI-V
    b. ManagementServer; Providing required parameters to associate the UNI-V with the ACS
    c. WANIPConnection; Providing information about the WAN interface (facing the ACS) on the UNI-V.
2) TR-104: Voice over IP provisioning data model; this defines the VoiceService and VoiceProfile on the UNI-V.

Details of each parameter supported by the UNI-V for the above data models are described in detail in sections 10.1 and 10.2.

5.2. DHCP and TR-069 Authentication

When the UNI-V boots up (e.g. first time boot), the following are discussed:

- UNI-V will initiate a DHCP discovery message across the NBN Co Network to access seeker's network.
- Once the DHCP discovery phase is complete, the UNI-V on the NTD is configured with its IP address and the ACS URL (other DHCP options are supported as set out above).
- UNI-V initiates communication with the ACS via TR-069 implementation.
- The UNI-V will use ProvisioningCode for both the HTTP username and password, if provided by DHCP
- The UNI-V will initiate a TR-069 HTTP POST request to the ACS with the HTTP password being hashed using the MD5 algorithm.
- Once the ACS confirms the identity and credentials of the UNI-V, a TR-069 session is established.
- Once the TR-069 session is established, the ACS can then make any other Remote Procedure Calls (RPC) that it requires to the UNI-V during this particular CWMP session (e.g. ACS uses SetParameterValues RPC to configure the UNI-V).

The TR-069 implementation on the UNI-V supports the use of HTTP digest authentication (using MD5 digest algorithm). The authentication can occur in both directions as follows:

- The UNI-V authenticates the ACS's Connection Requests.
- The ACS authenticates the UNI-V's session initiation.

Figure 2 illustrates an overview of DHCP and TR-069 traffic flow between the UNI-V and access seeker ACS.

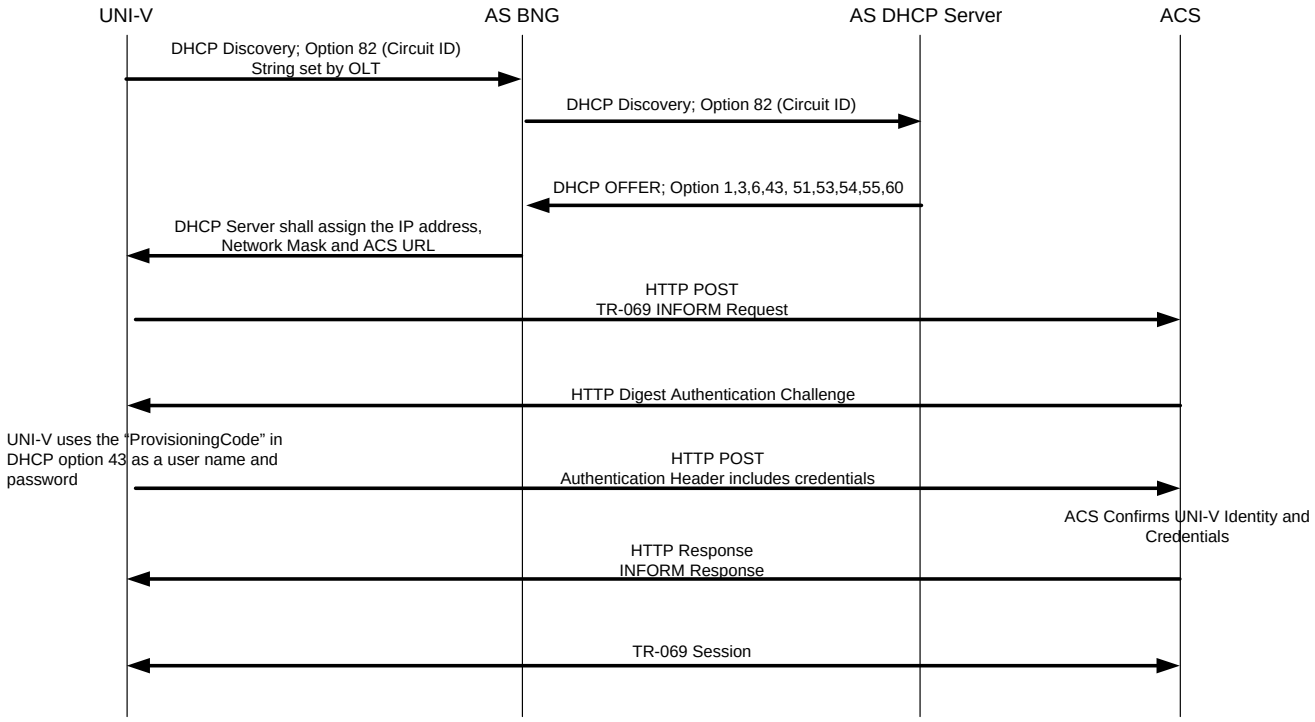


Figure 2 - DHCP and TR-069 authentication overview

5.2.1. ACS Discovery and Fail over Mechanism

The ACS URL and ProvisioningCode can be re-configured on the UNI-V through DHCP renewals in the following circumstances.

For example, if the ProvisioningCode that is initially configured on the UNI-V by access seeker (via DHCP Option 43) was incorrect, the UNI-V will not successfully authenticate with the ACS. To recover from this scenario, access seeker can correct the ProvisioningCode served by the DHCP server and wait for the next lease renewal. It is therefore important for access seeker to choose the DHCP lease time carefully to balance the DHCP server load and the time required to recover from configuration errors.

If access seeker configures the UNI-V with an incorrect ACS URL through the DHCP server or ACS, the UNI-V will retry to connect to the incorrect ACS URL for 300 seconds before it considers the ACS unreachable and fails back to the DHCP server by sending a DHCP REQUEST message. The DHCP server can configure the UNI-V with DHCP Option 43 that has the correct ACS URL.

Figure 3 - ACS Discovery and Fail over Mechanism, describes the traffic flow when the UNI-V is configured with an incorrect ACS URL.

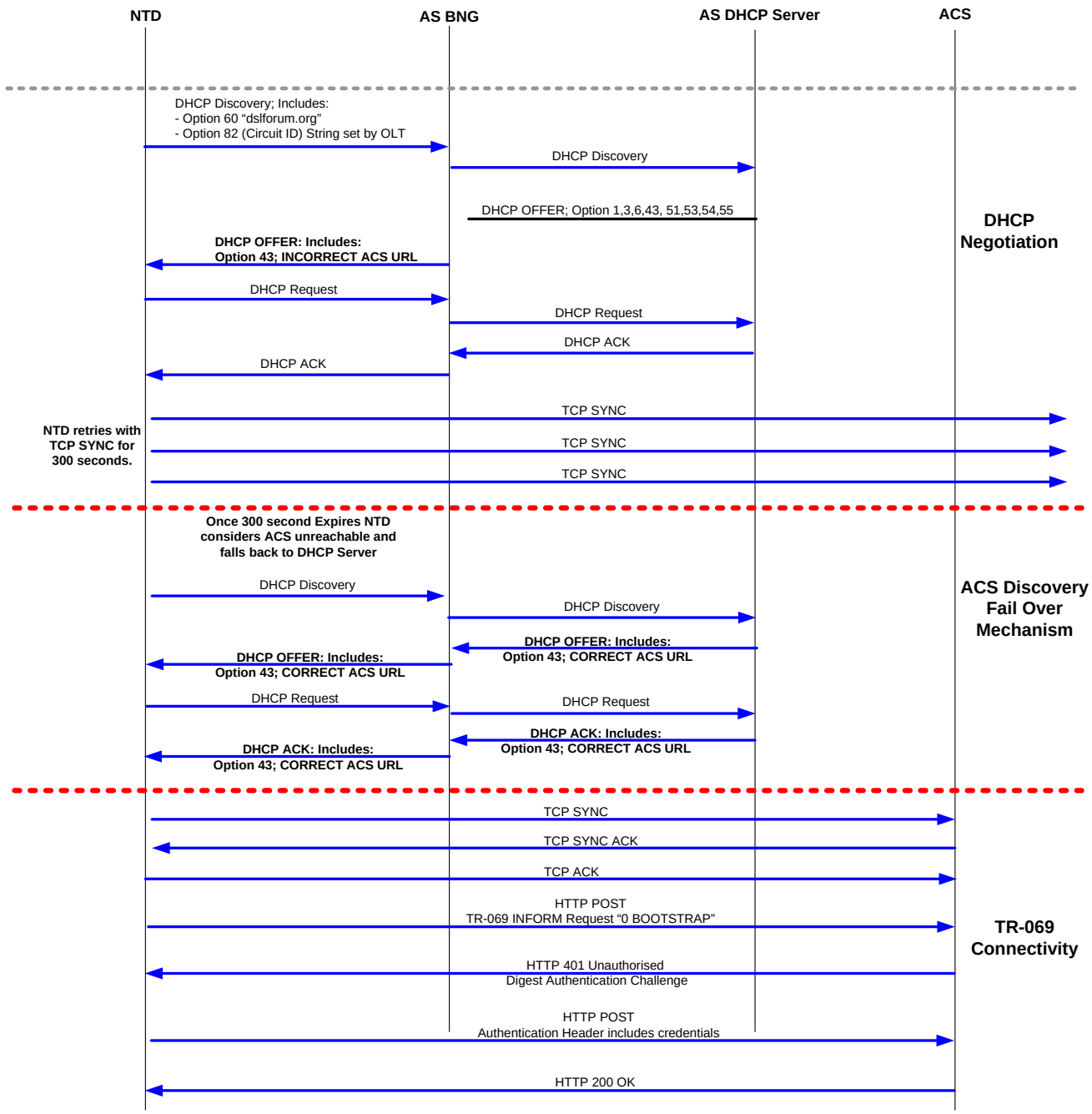


Figure 3 - ACS Discovery and Fail over Mechanism

5.3. Remote Procedure Call (RPC)

The CWMP client on the UNI-V uses RPC for communication between the ACS and the UNI-V (RPC can be used in both directions).

RPC Methods supported on UNI-V	ACS Requirement	Description
GetRPCMethods	Optional	Sent by the ACS to find out about the methods supported by the UNI-V.
GetParameterNames	Required	This method is used by the ACS to discover the UNI-V supported parameters.
GetParameterValues	Required	This method is used by the ACS to obtain the value of one or more UNI-V Parameters.
GetParameterAttributes	Optional	This method is used by the ACS to read the attributes associated with one or more UNI-V Parameter. Note that parameter attributes cannot be configured.
SetParameterValues	Required	This method is used by the ACS to modify the value of one or more of the UNI-V Parameters.
AddObject	Optional[1]	Adds a new VoiceProfile object instance on the UNI-V.
DeleteObject	Optional	Deletes a VoiceProfile object instance on the UNI-V.

Table 6 - Brief description of protocol layers

The table below sets out an example of the calling arguments of each of the RPC methods supported by the UNI-V and how access seeker may encode these arguments.

Note 1: Whilst optional from a TR-069 standards perspective, creation of the VoiceProfile object is required in order to provision a UNI-V service.

RFC Method	Encoded Message
GetRPCMethod	This RPC method has no calling arguments.
GetParameterNames	<cwmp:GetParameterNames xmlns:cwmp="urn:dslforum-org:cwmp-1-0"> <ParameterPath>InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.SIP.RegisterExpires</ParameterPath> <NextLevel>0</NextLevel> </cwmp:GetParameterNames>
GetParameterValues	<cwmp:GetParameterValues xmlns:cwmp="urn:dslforum-org:cwmp-1-0"> <ParameterNames SOAP-ENC:arrayType="xsd:string[1]" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"> <string>InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.SIP.RegisterExpires</string> </ParameterNames> </cwmp:GetParameterValues

GetParameterAttributes	<cwmp:GetParameterAttributes xmlns:cwmp="urn:dslforum-org:cwmp-1-0"> <ParameterNames SOAP-ENC:arrayType="xsd:string[1]" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"> <string>InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.SIP.RegisterExpires</string> </ParameterNames> </cwmp:GetParameterAttributes>
SetParameterValues	<cwmp:SetParameterValues xmlns:cwmp="urn:dslforum-org:cwmp-1-0"> <ParameterList SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"> <ParameterValuesStruct> <Name>InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.SIP.RegisterExpires</Name> <Value xsi:type="xsd:unsignedInt">3600</Value> </ParameterList> <ParameterKey></ParameterKey> </cwmp:SetParameterValues>
AddObject	<cwmp:AddObject xmlns:cwmp="urn:dslforum-org:cwmp-1-0"> <ObjectName>InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.</ObjectName> <ParameterKey>SyncAdd</ParameterKey> </cwmp:AddObject>
DeleteObject	<cwmp:DeleteObject xmlns:cwmp="urn:dslforum-org:cwmp-1-0"> <ObjectName>InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.</ObjectName> <ParameterKey>SyncAdd</ParameterKey> </cwmp:DeleteObject>

Table 7 - Examples of RPC Method encodings

5.3.1. Session Retry

The UNI-V will retry failed sessions to attempt to redeliver events or messages that it has previously failed to deliver and to allow the ACS to make additional requests in a timely fashion.

When a session fails, the UNI-V chooses the wait interval by randomly selecting a number of seconds from a range given by the post-reboot session retry count set out in
Table 8.

The UNI-V will execute the session retry table below in the following scenarios:

- If the UNI-V cannot establish a session to the ACS after a “0 BOOTSTRAP” has been successfully delivered.
- If the UNI-V failed to authenticate with the ACS with the correct username and password.

Post Reboot Session Retry Count	Wait Interval Range (Minimum-Maximum Seconds)
#1	5-10
#2	10-20
#3	20-40

Table 8 - Session Retry Wait Interval

5.4. INFORM events Supported

Each event is an 'INFORM' message sent from the UNI-V to the ACS. An event is an indication of an occurrence that requires the UNI-V to notify the ACS via an Inform request. The UNI-V will attempt to deliver every event at least once. If the UNI-V is not currently in a session with the ACS, it will attempt to deliver the event immediately; otherwise, the UNI-V will attempt to deliver the event after the current session terminates. The UNI-V will not consider an event successfully delivered unless it receives confirmation from the ACS. Once the UNI-V has delivered an event successfully, the UNI-V will not send the same event again.

When the UNI-V sends an INFORM event to the ACS and does not receive a response back, after a time interval the UNI-V will re-send the event again as described in
Table 8. Therefore access seeker must ensure the ACS is prepared to receive the same event more than once.

5.4.1. 0 - BOOTSTRAP

The “0 BOOTSTRAP” event code is supported on the UNI-V once a session is established between the UNI-V and ACS to specify the event of a first-time NTD installation, UNI-V activation or a change to the ACS URL.
This event code will be triggered in the following use case scenarios:

- Upon the connection of a new NTD or the replacement of a current NTD with a new one.
- Upon the user manually setting the NTD to “factory reset” (using factory reset button on the NTD). Note the UNI-V does not allow the ACS to execute a factory reset remotely.
- Upon connection between the UNI-V and ACS after access seeker has modified the ACS URL address.
- Upon changing the value of option code 254 in DHCP Option 43. Refer to section 3.2.1.1 of this document for further details.

On “0 BOOTSTRAP”, the ACS may configure the UNI-V with the username and password which is then stored and used for subsequent digest authentication of ACS Connection Requests.

5.4.2. 1 - BOOT

The “1 BOOT” event code is supported on the UNI-V when a session is established between the UNI-V and ACS specifying NTD system reboot. This event code will be triggered upon manual reboot of NTD by the End User.
The “Reboot” Remote Procedure Method and the “M Reboot” event code are not supported by the UNI-V.

5.4.3. 2 - PERIODIC

The “2 PERIODIC” event code is supported on the UNI-V when a session is established. It specifies that the session was initiated due to Periodic Inform Interval attribute being set by the ACS.
Access seeker can enable/disable the periodic interval attribute and set its value via the ACS meaning the UNI-V will contact the ACS periodically.

5.4.4. 6 - CONNECTION REQUEST

The “6 CONNECTION REQUEST” event indicates that the session was established due to a connection request initiated by the ACS.

This event is a very important code as it will be utilised in every use case scenario where the ACS initiates a connection to the UNI-V. The event uses HTTP GET destined to the UNI-V URL and the UNI-V will use digest authentication to authenticate the ACS before sending a 200 OK response.

Access seeker must ensure that the ACS supports the connection request method to prompt the UNI-V to immediately contact the ACS. This may be required when voice service parameters need changing e.g. modification of a voice service.

5.4.5. Advertising UNI-V IP Address to ACS

The UNI-V advertises its current IP address to the access seeker ACS under the following scenarios:

- The first time it connects to the ACS (“0 BOOTSTRAP” inform)
- On subsequent connections from a power up or reboot (“1 BOOT” inform)
- On every “PeriodicInformInterval” (periodic inform)
- On every “6 CONNECTION REQUEST” triggered by the ACS.

5.5. Unsupported INFORM events

The following event codes specified in TR-069 are not supported by the UNI-V:

- 3 - SCHEDULED
- 4 - VALUE CHANGE (Although this parameter is displayed in the “0 BOOTSTRAP” event code, it is not supported)
- 5 – KICKED
- 7 - TRANSFER COMPLETE
- 8 - DIAGNOSTICS COMPLETE
- 9 - REQUEST DOWNLOAD
- M -REBOOT
- M - DOWNLOAD
- M - UPLOAD
- M - VENDOR SPECIFIC METHOD
- M - VENDOR SPECIFIC EVENT
- M – SCHEDULEINFORM

5.6. UNI-V Responses to ACS Requests

The UNI-V will respond to the ACS requests with message responses that are dependent on the use case. Table 9 sets out the responses that the UNI-V will generate depending on the request received by the ACS.

UNI-V Response Messages Supported	Request by the ACS	Description
Event code: BOOTSTRAP, BOOT, PERIODIC and CONNECTION REQUEST. All these event codes will include "Authorisation" header	ACS challenges the UNI-V with "HTTP 401 Unauthorized".	When the ACS sends a challenge to any of the event codes generated by the UNI-V, the UNI-V will respond with the same event code (being challenged) including an "Authorization" header that has the username and password.
6 CONNECTION REQUEST	ACS sends a HTTP GET to trigger the UNI-V to communicate to the ACS	The UNI-V will always respond with CONNECTION REQUEST. This is used, for example, if the ACS is required to implement the configuration of a parameter on the UNI-V.
HTTP POST- empty	ACS authenticates the UNI-V successfully by sending HTTP 200 OK.	The UNI-V has no further requests to send to the ACS and the UNI-V has issued an empty HTTP POST to the ACS. The ACS will respond (if there are no further requests to implement) with HTTP 204 NO CONTENT.
HTTP POST SetParameterValuesResponse <Status>0<Status>	ACS sends HTTP response with "SetParameterValues" method for one or multiple of parameters.	The UNI-V has acted upon the "SetParameterValues" sent by the ACS and hence will send a response to confirm successful execution.
HTTP POST GetParameterValuesResponse <Name>"parameter_name"</Name> <Value>parameter_value_set</Value>	ACS sends HTTP response with "GetParameterValues" method for one or multiple of parameters.	The UNI-V responds by transmitting all requested parameter names and the value setting of each parameter.
HTTP POST GetParameterNamesResponse <Name>"parameter_name"</Name> <Writable>"Read-Or-Write"</Writable>	ACS sends HTTP response with "GetParameterNames" method for one or multiple of parameters.	The UNI-V responds by displaying all requested parameter names and whether each parameter can be configured using the SetParameterValues method.
HTTP POST AddObjectResponse <InstanceNumber>New_Object_Number</ InstanceNumber> <Status>Creation_Status</Status>	ACS sends HTTP response with "AddObject" method to create the VoiceProfile Object.	The UNI-V responds with the instance number of the newly created VoiceProfile object and the status specifying that the VoiceProfile has been created successfully.
HTTP POST DeleteObjectResponse <Status>Deletion_Status</Status>	ACS sends HTTP response with "AddObject" method to delete the VoiceProfile Object.	The UNI-V responds with the status specifying that the VoiceProfile has been deleted successfully or has been committed but not yet applied.

Table 9 - Response Message Codes supported on the UNI-V TR-069 Protocol Layer

6. TR-069 Use Case Scenarios

This section illustrates possible use cases and the requests/responses which the UNI-V supports in each use case.

The following use cases are described in this section:

- NTD First time boot (i.e. at initial installation), eg, because of:
  - Manual factory reset (i.e. by the End User)
  - Remote reset of the UNI-V by NBN Co (Access seeker may request this of NBN Co by raising a trouble ticket).
  - NTD Replacement.
- NTD manual reboot (i.e. by the End User).
- Change voice service on NTD.
- Cancel voice service on NTD.
- TR-069 Authentication failed - Incorrect HTTP Password.

6.1. Use Case 1: NTD First Time Boot.

At initial boot up, the NTD will only have the factory default configuration from the manufacturer. This will include the following:

- Country code VoIP generic configuration
- NTD hardware specific configuration

This is also the case in the following scenarios:

- Manual factory reset (i.e. by the End User)
- Remote reset of the UNI-V by NBN Co (Access seeker may request this of NBN Co by raising a trouble ticket).
- NTD replacement.

Figure 4 illustrates the DHCP and TR-069 traffic flow when a new NTD is installed.

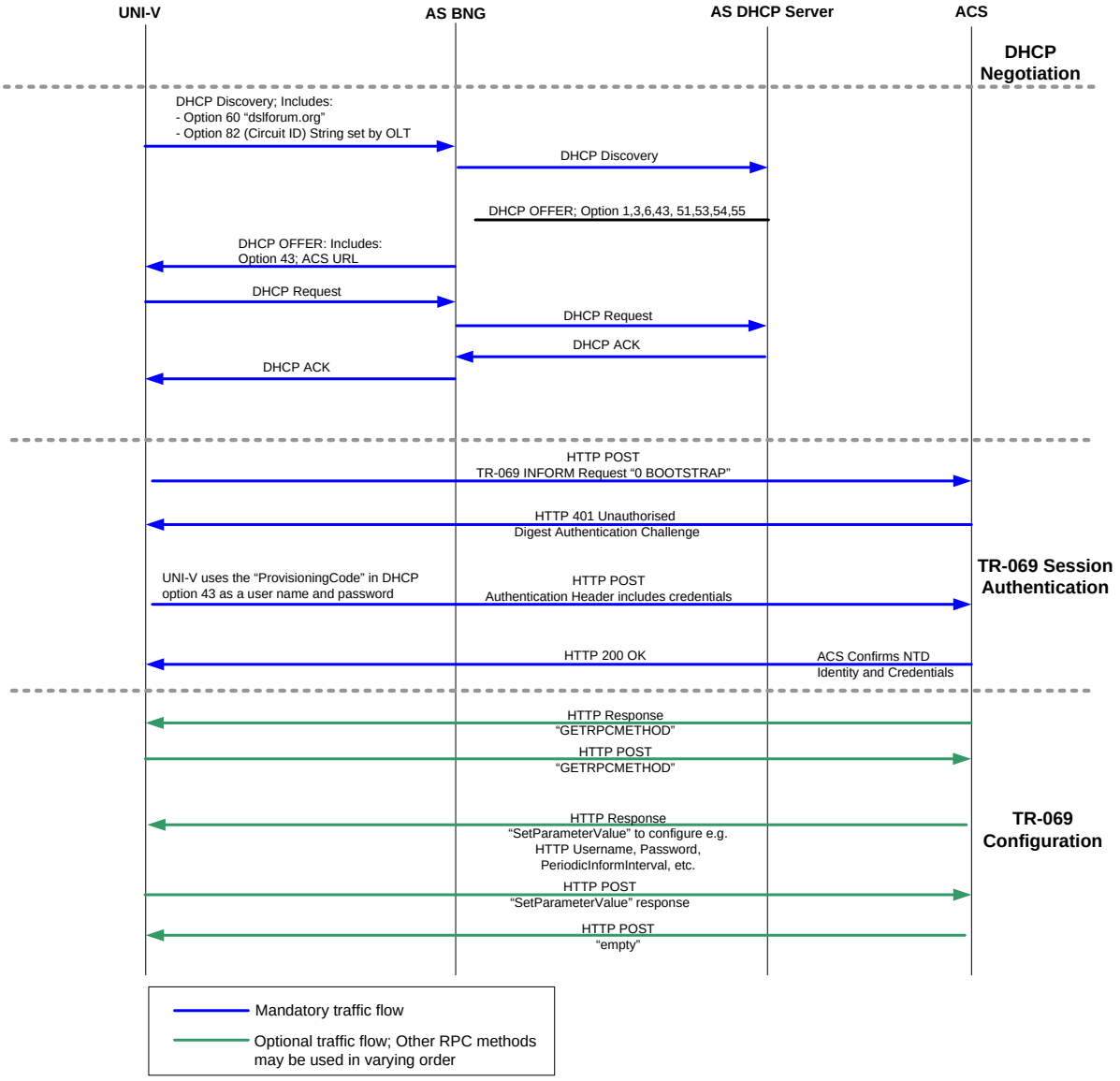


Figure 4 - DHCP & TR-069 Traffic Flows

Once the NTD has booted up, the following sequence of events will take place:

1) The UNI-V will send a DHCP discovery message to the access seeker DHCP server with option 82 (circuit ID) being set by the OLT.
2) Once the DHCP configuration phase is completed, the UNI-V will be configured with IP address and network mask, ACS URL (DHCP Option 43) and DNS Server address.
3) The UNI-V resolves the ACS URL using the DNS Server and initiates a "6 CONNECTION REQUEST" (HTTP POST) to the ACS. The UNI-V sends a "0 BOOTSTRAP" INFORM message. The INFORM message will contain the following CWMP information in the <cwmp: Inform> header:

DeviceId (Manufacturer, NTD Serial number, OUI and ProductClass). The values are set as follows:

- Manufacturer; set to "**ALCL**" (indicating Alcatel-Lucent).
- OUI; set to "**0019C7**".
- SerialNumber; this is the serial number of the UNI-V configured by DHCP option 43 option code 254.
- ProductClass; this is the NTD variant, i.e. Indoor "**I-240G-R**" or Outdoor "**O-240G-P**".

Event:

- "0 BOOTSTRAP"
- "4 VALUE CHANGE" (Although this parameter is displayed in the "0 BOOTSTRAP" event code, it is not supported)

ParameterList:

- InternetGatewayDevice.DeviceInfo.SpecVersion
- InternetGatewayDevice.DeviceInfo.HardwareVersion
- InternetGatewayDevice.DeviceInfo.SoftwareVersion
- InternetGatewayDevice.DeviceInfo.ProvisioningCode
- InternetGatewayDevice.DeviceInfo.ParameterKey
- InternetGatewayDevice.DeviceInfo.ConnectionRequestURL
- InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.ExternalIPAddress
- InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.MACAddress

4) The ACS sends an authentication challenge to the UNI-V using "401 Unauthorized".
5) The UNI-V then responds with an HTTP response including "Authorization" header. The header includes the HTTP credentials configured by DHCP option 43.
6) The ACS confirms the UNI-V identity by checking the HTTP credentials. Access seeker must ensure these HTTP credentials (i.e. set by the "ProvisioningCode") have been pre-defined for each device type in the ACS.
7) The ACS then identifies the UNI-V by looking at the "DeviceId" and confirming the "Serial Number" **(configured via DHCP option 43 option code 254)** and "Manufacturer OUI" of the UNI-V (optionally the ACS may also use the ProductClass).

8) After the ACS confirms the NTD is a new device, the ACS may send a “SetParameterValue” action to configure the UNI-V: Eg:
    - HTTP username: InternetGatewayDevice.ManagementServer.Username
    - HTTP password: InternetGatewayDevice.ManagementServer.Password
    - UNI-V INFORM periodic interval: “InternetGatewayDevice.ManagementServer.PeriodicInformInterval”.
    - Connection Request Password: “InternetGatewayDevice.ManagementServer.ConnectionRequestPassword”
    - Connection Request Username: “InternetGatewayDevice.ManagementServer.ConnectionRequestUsername”
9) The UNI-V replies with a “SetParameterValueResponse” message, for acknowledgement.
10) Every time the UNI-V receives a connection request from the ACS (HTTP GET) the UNI-V first challenges the ACS with “401 Unauthorized” to confirm the ACS identity. The ACS must then authenticate with the UNI-V using the HTTP credentials, i.e. “ConnectionRequestUsername” and “ConnectionRequestPassword” as configured in step 8) above.
11) When the UNI-V initiates a “6 CONNECTION REQUEST”, the ACS must challenge the UNI-V with “401 Unauthorized”. The UNI-V will respond by sending an Inform Message to the ACS with its HTTP credentials.
12) The ACS may query the UNI-V for its supported RPC method capabilities, using the “GetRPCMethod”.
13) The UNI-V responds with “GetRPCMethodsResponse” including the RPC methods it supports.

Figure 5 illustrates TR-069 traffic flow to create a voice profile object.

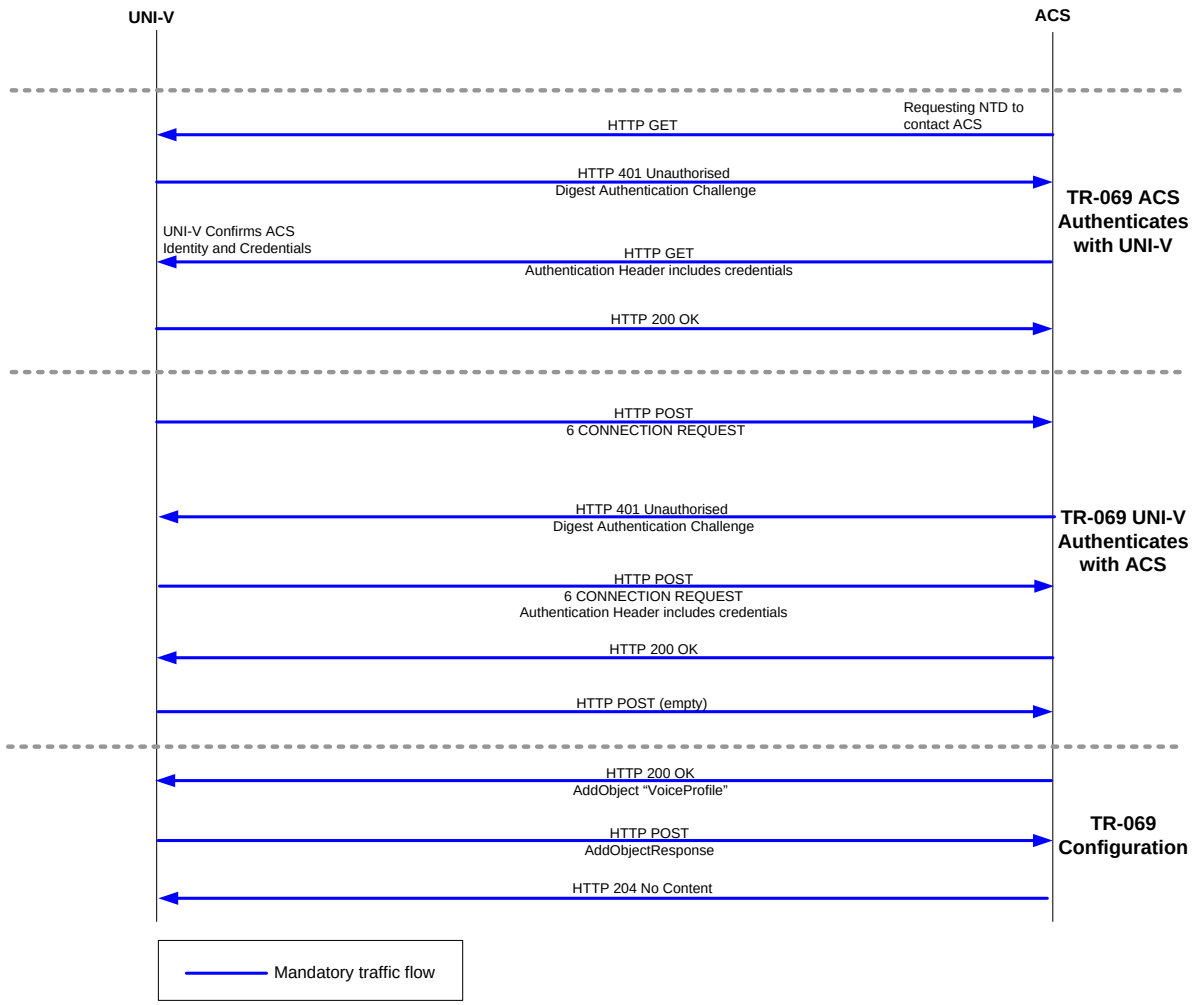


Figure 5 - Add VoiceProfile Object

14) To configure a new voice service, the ACS must first send the message “AddObject” to create InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}. The UNI-V will automatically also create a Line object.
15) The UNI-V, upon creating the object successfully, responds with “AddObjectResponse” with VoiceProfile object instance set “1”.
16) The ACS uses the “SetParameterValue” method to configure the “InternetGateway Device.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}” object parameters as shown in Figure 6.

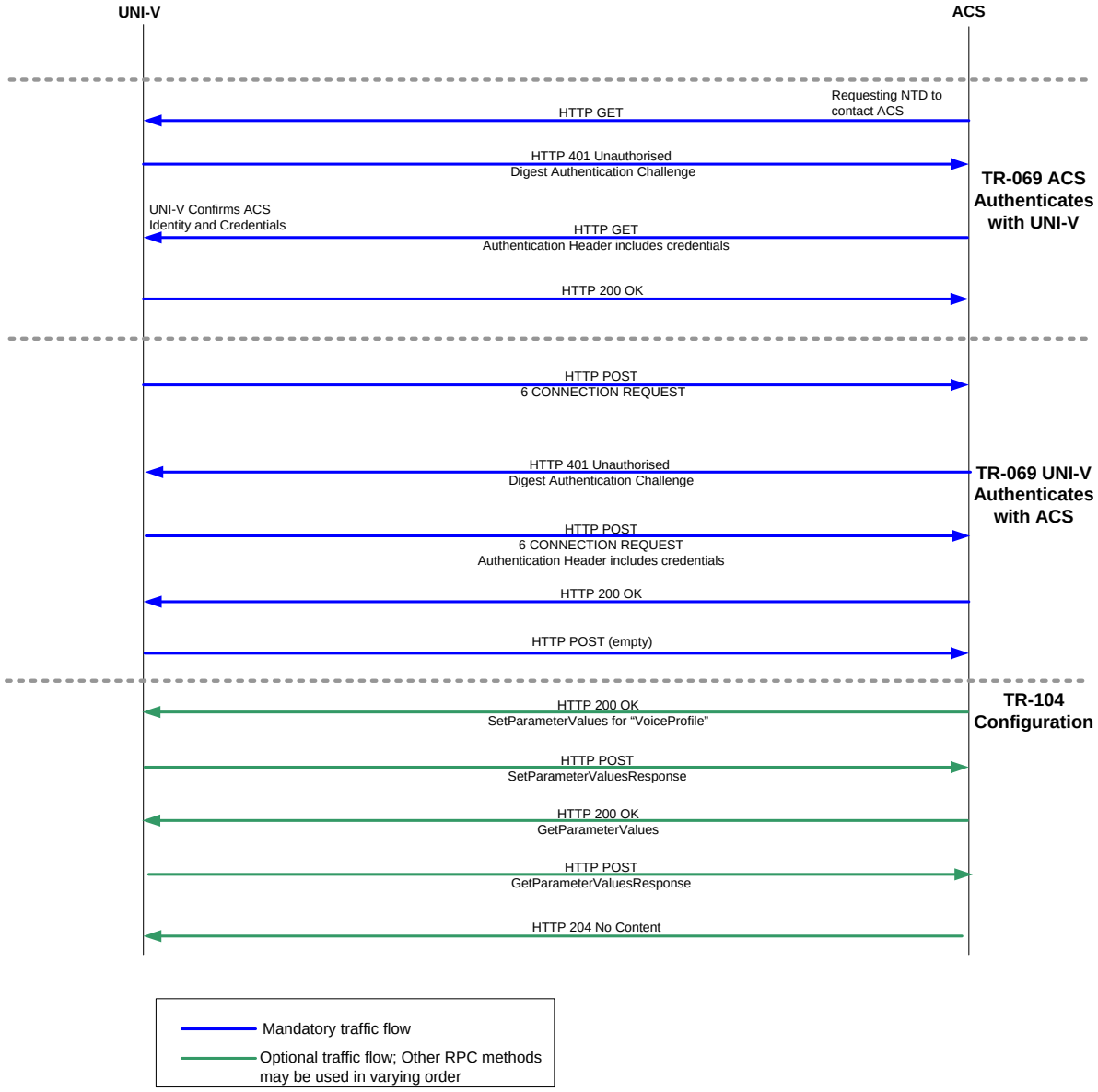


Figure 6 - Configure a new Voice Service

17) Every time the ACS sends a "SetParameterValue" to configure a parameter on the UNI-V, the UNI-V replies with a "SetParameterValueResponse" message, for acknowledgement (to confirm parameter value has been configured).

18) Once the ACS completes the provisioning, it will send an empty TR-069 message to indicate session closure (i.e. HTTP 204 No Content).

6.2. Use Case-2 NTD Manual Reboot

If the End User manually reboots the NTD, steps 1 to 5 in section 6.1 will be executed first with the exception that step 3 will not include “0 BOOTSTRAP” event code.

The following events then take place:

1) The UNI-V will send an INFORM message with a “1 BOOT” event code that informs the ACS a manual reboot has occurred.
2) The ACS confirms the UNI-V identity by checking the HTTP username/password.
3) Since the UNI-V sent an INFORM message with a “1 BOOT” event code, the ACS recognises this is a reboot event and that it does not need to configure the UNI-V (e.g. no TR-104 SIP configuration required). SIP configuration on the UNI-V will still be available after the reboot.

6.3. Use Case-3 Modification of End User Voice Service

This use case occurs when an access seeker wishes to modify a specific Customer Product being supplied to an End User, for example this includes the following changes:

- Adding/Removing a supplementary voice service for an End User
- Changing SIP username/password for an End User
- Changing a SIP configuration for an End User

The above service modifications do not require the voice service to be relinquished or removed. Adding or removing Customer Product voice features will not impact the voice service at the NBN Co Product level.

The sequences of events that are implemented to modify a voice service are as follows:

1) The ACS initiates a connection request (HTTP GET) to the UNI-V.
2) The UNI-V challenges the ACS with “401 Unauthorized”.
3) The ACS then authenticates using the HTTP credentials, i.e. “ConnectionRequestUsername” “ConnectionRequestPassword”.
4) The UNI-V verifies the ACS identity.
5) The UNI-V responds with HTTP message with “6 CONNECTION REQUEST” as an event code.
6) The ACS challenges the UNI-V with “401 Unauthorized”.
7) The UNI-V will responds by sending an Inform Message to the ACS with HTTP credentials.
8) The ACS verifies the UNI-V identity.
9) The ACS sends “SetParameterValue” to set the required parameter changes.
10) The UNI-V replies with a “SetParameterValueResponse” for acknowledgement.

6.4. Use Case-4 Cancellation of End User Voice Service

If the access seeker no longer desires to a provide a voice service to the End User, it may disconnect the UNI-V in accordance with the processes set out in the NBN Co Operations Manual and the access seeker’s access to the UNI-V and related NFAS Product Components will be removed.

6.5. Use Case-5 UNI-V Authentication failure with the ACS

If the UNI-V has an incorrect HTTP password, the connection will be rejected by the ACS and the UNI-V will keep retrying at random intervals from a range given by the post-reboot session retry count. See section 5.3.1.

6.6. Use Case-6 UNI-V Network Connectivity failure with the ACS

When an UNI-V is configured with a new ACS URL (via DHCP Option 43 or via ACS TR-069 configuration), the UNI-V will connect to the URL by sending “0 BOOTSTRAP”.

If the UNI-V fails to connect to the ACS within 300 seconds, the UNI-V will fall back to the DHCP server, requesting a new DHCP offer and will continue to cycle until a successful connection to the ACS is achieved. This is described in more detail in section 5.2.1.

7. TR-104 Diagnostic Parameters Supported

Access seeker's ACS can query the UNI-V using TR-069 RPC methods to retrieve information about the connection or service status using the UNI-V voice line status in accordance with TR-104.

The UNI-V voice line object supports the following diagnostic parameters under the InternetGatewayDevice.Services .VoiceService.VoiceProfile.Line object:

- Status: Indicates the status of the UNI-V. For example if the status is "Up" this indicates the UNI-V is successfully registered with the access seeker's softswitch.
- CallState: Indicates the current status of the connection to the UNI-V, e.g. Idle, InCall, Calling, etc.

8. UNI-V SIP Overview

The UNI-V SIP client will control the analogue states of the UNI-V, detect and process dialling, generate tones and Caller ID FSK transmissions, while signalling with the softswitch to control the phone call, and establish/tear down the RTP bearer channel associated with the voice path.

Signalling flows occur between the UNI-V and the softswitch. UNI-V traffic is carried in RTP packets which flow through the NBN Co Network in the same AVC as the signalling packet flow.

The UNI-V is an intelligent client (TISPAN Loosely Coupled), meaning it locally processes hook-flash events and the call-waiting service logic without reporting the hook-flash event to access seeker's softswitch. The UNI-V's call-waiting service logic may trigger the sending of SIP messages to access seeker's softswitch (e.g. placing an existing call on hold). Call feature service logic not utilising hook-flash events can also be implemented on access seekers' softswitch using basic SIP functions from RFC3261 with a single signalling dialog for a voice call.

8.1. UNI-V SIP Standards Support

The UNI-V SIP stack on the NTD is based on the SIP standards listed in Table 10:

SIP Standard Supported on indoor and outdoor NTDs	Definition
RFC3261	Session Initiation Protocol (**SIP**)
RFC2327	Session Description Protocol (**SDP**)
RFC3264	An offer/answer model with Session Description Protocol (**SDP**)
RFC3550	RTP: A transport protocol for real-time applications

Table 10 - UNI-V SIP Standard support

8.1.1. UNI-V SIP Extension Standards

Table 11 sets out the SIP extension standards supported or partially supported on the UNI-V and describes how these standards apply in relation to the UNI-V.

SIP extension standard supported on NTDs	Description
RFC3262: Reliability of provisional responses in SIP	The UNI-V supports and inserts a 100Rel header field for new requests.
RFC3265: SIP specific event notification	Used for Message Wait Indication
RFC3311: SIP UPDATE method	May be used like a re-INVITE to modify SDP properties
RFC3325: Private extensions to the SIP for asserted identity within trusted networks	This standard is utilised in some cases for caller ID information. This is not generated by the UNI-V
RFC3842: A message summary and message waiting indication event package for SIP	Used with Message Waiting Indication
RFC3515: SIP	This includes support for NOTIFY messages
RFC3611: RTP Control Protocol Extended Reports (RTCP XR)	The VoIP metric report block is the only supported report. Other reports are not supported.
RFC3960: Early media and Ringing Tone generation in SIP	The UNI-V will accept early media using Gateway model for both modes

Table 11 - UNI-V SIP Extension Standards Support

Table 12 illustrates the SIP methods and requests supported on the UNI-V SIP stack as per the SIP RFCs mentioned above.

SIP methods supported	Definitions
REGISTER	Registers a UNI-V with a softswitch
INVITE	Establishes a new call or updates properties of an active call
UPDATE	Used to modify the properties of a call
PRACK	Reliable acknowledge for intermediate answers during call setup
OPTIONS	Used by the softswitch to verify connectivity with the UNI-V and query its capabilities
ACK	Final response message to a request
BYE	Ends a call
CANCEL	Cancels a request transaction prior to 200 OK being received

Table 12 - SIP Method and Request Messages Supported on the UNI-V SIP Stack

Response codes are used as intermediate responses or final responses to SIP requests. The response codes supported specifically by the UNI-V are listed in Table 13.

All other 3xx, 4xx, 5xx, and 6xx SIP response codes received by the UNI-V indicate that the request failed. In most cases, this will result in a feature tone output from the UNI-V to connected CE (e.g. Ringing, Busy Tone, etc.).

SIP response code	Action by UNI-V when receiving response code	Action when response code sent by UNI-V
100 Trying	No special action.	Sent in immediate response to an INVITE
180 Ringing	Send Ring-Back Tone to the UNI-V port	Sent in response to INVITE when a new call transaction is accepted by the UNI-V
183 Session Progress	If SDP included, establishes early media during call establishment. If no SDP, send Ring-Back Tone to the UNI-V port	Not sent by UNI-V
401 Unauthorized	UNI-V will re-try with authentication information	Not sent by UNI-V
403 Forbidden	Request/transaction failure	Not sent by UNI-V
407 Proxy Authentication Required	UNI-V will re-try with authentication information	Not sent by UNI-V
408 Request Timeout	Request/transaction failure	Cancels a received INVITE when a new call is not answered after internal UNI-V timeout
423 Interval Too Brief	Next Registration attempt will set the Registration Expires timer to 3600 seconds.	Not sent by UNI-V
488 Not Acceptable Here	Request/transaction failure	An SDP offer did not contain any Codec configured for the SIP service
486 Busy	End transaction; send Busy Tone to the UNI-V port	Sent in response to INVITE when a new call can't be accepted
491 Request Pending	Request/transaction failure	Sent when a transaction in the same dialog is already in progress

Table 13 - Response Message Codes Supported on the UNI-V SIP Stack

8.1.2. Codec Negotiation

Codec negotiation is performed using the SDP offer / answer model (RFC3264).

The SDP offer is contained in the INVITE and the SDP answer is contained in the INVITE "200 OK" response:

- When the UNI-V originates a call the INVITE sent to access seeker's softswitch contains SDP with a priority list of all codecs supported by the UNI-V.
- If the UNI-V receives an INVITE with an SDP codec list that does not match any of the codecs supported by the UNI-V, the UNI-V will immediately after the "100 trying" send a "488 Not Acceptable Here" response to the INVITE.
- When an incoming call to the UNI-V is answered by an End User, the 200 OK response contains SDP for the highest priority codec received in the INVITE that is also supported by the UNI-V.

Either end of the call can renegotiate the codec being used, in mid–call, by initiating a subsequent SDP offer / answer exchange using a REINVITE and "200 OK" response.

For SDP codec negotiation the SIP "Content-Type" supported is "application/sdp".
The UNI-V does not support the receipt of multipart SIP bodies.

8.1.3. UNI-V SIP Timers supported

This section sets out the timers supported on the UNI-V for basic SIP signalling messages.

SIP timer parameter	Timer description	Value	access seeker configuration privilege level
Registration Expires	The registration expiration time that the client will propose by including it in an "Expires" header of a REGISTER request	default 3600 seconds	Configurable in TR-104
Register retry timer	The duration to wait after a failed registration attempt (including the RFC3261 defined retries) and the next registration attempt	30 seconds	Not configurable in TR-104
RegistrationPeriod	RegistrationPeriod is the interval at which UNI-V will send re-REGISTER messages. It is configurable and should be less than or equal RegisterExpires.	default 3240 seconds	Configurable in TR-104.

Table 14 - UNI-V SIP Registration Timers

- At NTD reboot, a random registration delay (0 to 5 minutes) is calculated and initiated. This delay is implemented to alleviate registration storms.
- UNI-V Registration Period values chosen should be consistent with the access seeker softswitch minimum registration period. If the UNI-V registration period value is lower than this time, access seeker's softswitch may send a "423 Interval Too Brief" response. On receipt of a 423 registration response the UNI-V will resend the Registration request with the registration "Expires" header set to 3600 seconds.
- By default, the UNI-V renews its registration 360 seconds before the current registration expires (configurable in TR-104).
- When determining the TR-104 "Registration Period" and "RegisterExpires" values, NBN Co recommends that access seeker balances the values which affect the End User's service recovery time with minimising registration traffic which has the potential to generate registration storms.
- The Register retry timer is set to 30 seconds and is not a configurable parameter.

The following timers are built in the firmware of each NTD, are defined in accordance with RFC3261 and are not configurable by access seeker.

SIP timer parameter	Description
Invite message timer	The INVITE transaction timeout, designated as Timer B in RFC3261
Non-INVITE message timer	The non-INVITE transaction timeout, designated as Timer F in RFC3261
sip_timer_t2	The value of the SIP T2 timer (the maximum retry interval for a non-INVITE request)
sip_timer_t1	The value of the SIP T1 timer (the round-trip time estimate)

Table 15 - UNI-V SIP Timers

8.1.4. Digit collection timers

The digit collection timers are controlled by NBN Co and are set to:

- First digit timer - 12 seconds (+/- 0.5 seconds)
  This is the maximum time allowed between a telephony device connection to the UNI-V going off-hook and the first digit being received. During this period Dial Tone is played. When the timer expires, Busy Tone is played.
- Inter-digit timer - 6 seconds (+/- 0.5 seconds)
  The maximum time allowed between digits. Applies to digit map patterns with and without the "T" symbol. Timer expiry indicates end of dialling. The # digit can also be used to indicate end of dialling.

8.1.5. Tones Support

The UNI-V supports the generation of the tones described in Table 16:

Tones supported	Tones triggers
Busy Tone	Transaction failure errors 4xx (except 404), 5xx, and 6xx in response to INVITE
Disconnect Tone	BYE received
Number Unobtainable Tone	Error 404 in response to INVITE
Call Waiting Tones	Call Waiting service logic
Dial Tones	UNI-V off-hook is detected
Message Waiting Indication Tone; Stutter Tone	Message waiting is active and off-hook is detected
Recall Dial Tone	Output by UNI-V when flash-hook is used and after dialling some service codes
Ringing Tone	180 Ringing message in response to INVITE

Table 16 - UNI-V SIP Tones

8.1.6. Dial Plan configuration

Dial Plan support on the UNI-V is implemented using a digit-map generally following the MGCP standard format. The Dial Plan string length can be up to 1024 characters including parenthesis. Guidelines and examples of configurations are set out below:

1) The following characters are valid as per the MGCP standard:

    a. Numeric number: 0,1,2,3,4,5,6,7,8,9.
    b. Character: *,#,(,), [,], |and .
    c. [ ] specifies the valid digit range. For example [1-5] indicates only the numbers 1 through 5 are acceptable.
    d. Arbitrary number(s): “x” or “x.”; Note that “x.” represents a numeric string of any length, including a length of 0.
    e. Timer: T; This is a critical dial timer, and there may be more than one T timer in the Dial Plan table. E.g. (123x.T|456x.T|**xxx.T). If any other character is included in the Dial Plan, the UNI-V will treat the whole Dial Plan as invalid and reject it.

2) The Dial Plan begins with “(“and ends with “)”. Each item in the Dial Plan is delimited by “|”. E.g. (1234|**##|x.T).

    The Dial Plan is configured using a string of up to 1024 characters including parenthesis E.g.(**xxx|000E|106E|***xx|*xx*x.*x#|*xx*x.*xx#|*xx*x.*x#|*31*xxxxxxxx|*xx#|#xx#|*#xx#|#001|x.T) The Dial Plan is applied to the End User service as per the details in to section 10.2.

3) Default Dial Plan
    The UNI-V uses its default Dial Plan in the case where there is no other Dial Plan or an invalid Dial Plan is configured. E.g. default Dial Plan would be:
    (***xx|*xx*x.#|*xx*x.*xx#|*xx*x.*x#|*31*xxxxxxxx|*xx#|#xx#|*#xx#|#001|x.T)

4) Matching rules
    Consider the default Dial Plan example below:
    (***xx|*xx*x.#|*xx*x.*xx#|*xx*x.*x#|*31*xxxxxxxx|*xx#|#xx#|*#xx#|#001|x.T)
    a. If one unique item is matched without ambiguity, the UNI-V will send the dialled numbers immediately. E.g. dial *43# matches the rule “|*xx#|”.
    b. If the matched item contains timer T, UNI-V will delay initiating a call until the timer has expired. If a new digit is dialled before the timer expires, the UNI-V will re-check the dialled number containing new digits to see if the dialled number matches. E.g. dial 123456 matches the rule “|x.T|”.
    c. If the dialled numbers do not match any items, the UNI-V will not send the numbers. E.g. dial ***# .
    d. If the numbers dialled match more than one item, the UNI-V will match on the item with the least number of wildcards to match. E.g. (***xx|123xxx.T|1234)
    After dialing 1234, the UNI-V will initiate a call as the rule item1234 was matched instead of 123xxx.T.

Note: access seeker may specify service codes supporting call features based on the matching rules above.

Feature activation codes for the UNI-V's "Suspend Call Waiting" service (*70) and softswitch-based voice features such as Calling Number Display, call forwarding on busy, call forwarding on no answer and call forwarding unconditional, need to be included by access seeker in the digit map.

8.1.7. Real Time Control Protocol Support (RTCP)

The UNI-V supports Real Time Control Protocol as per RFC3550. The RTCP message provides "RTCP Sender Report" that includes the following parameters described in Table 17 but note this is not the exhaustive list.

RTCP Sender Report	RFC3550 Description
Sender's Packet Count	The total number of RTP data packets transmitted by the sender since starting transmission up until the time this SR packet was generated.
Sender's Octet Count	The total number of payload octets (i.e., not including header or padding) transmitted in RTP data packets by the sender since starting transmission up until the time this SR packet was generated.
Fraction Lost	The fraction of RTP data packets from the source lost since the beginning of reception. This is calculated by determining the number of packets lost divided by the total number packets sent.
Cumulative number of Packets lost	The total number of RTP data packets from source SSRC_n that have been lost since the beginning of reception. SSRC_n The SSRC identifier of the source to which the information in this reception report block pertains.
Interarrival jitter	An estimate of the statistical variance of the RTP data packet interarrival time measured in timestamp units and expressed as an unsigned integer.
Delay since last Sender Report (SR)	The delay, expressed in units of 1/65536 seconds, between receiving the last SR packet from source SSRC_n and sending this reception report block.

Table 17 - Examples of RFC3550 parameters supported by the UNI-V

When the call session is terminated, the NTD will send an RTCP BYE packet indicating that the call is no longer active. The RTCP BYE packet will include a constant "Goodbye (203)" in the "Packet type" identifying this to be a RTCP BYE message.

The VoIP metric report block is the only supported report and is included in the RTCP Header (RFC3611). Note that all other reports in RFC3611 such as Loss RLE report, Duplicate RLE report, Packet Receipt Times report, Receive Reference Times report, DLRR report and Statistics Summary report are not supported.

The VoIP Metrics Report Block provides metrics for monitoring VoIP calls. These metrics include packet loss and discard metrics, delay metrics, analogue metrics, and voice quality metrics.
When the NTD establishes a call connection and RTP traffic flows, the NTD will also start generating RTCP traffic to the other RTP endpoint. RTCP packets are transmitted every 5 seconds by the NTD (not configurable).

Table 18 below illustrates the VoIP metrics report block parameters supported by the NTD.

VoIP Metric Parameter	RFC3611 Description
Fraction Lost	The fraction of RTP data packets from the source lost since the beginning of reception. This is calculated by determining the number of packets lost divided by the total number packets sent.
Fraction Discarded	The fraction of RTP data packets from the source that have been discarded since the beginning of reception, due to late or early arrival, under-run or overflow at the receiving jitter buffer. This is calculated by determining the number of packets discarded divided by the total number of packets expected.
Burst Density	The fraction of RTP data packets within burst periods since the beginning of reception that was either lost or discarded. This is calculated by determining the total number of packets lost or discarded within the burst periods divided by the total number of packets expected.
Gap Density	The fraction of RTP data packets within inter-burst gaps since the beginning of reception that was either lost or discarded.
Burst Duration	The mean duration, expressed in milliseconds, of the burst periods that have occurred since the beginning of reception.
Gap Duration	The mean duration, expressed in milliseconds, of the gap periods that have occurred since the beginning of reception.
Round Trip Delays	The most recently calculated round trip time between RTP interfaces, expressed in milliseconds.
End System Delay	The most recently estimated end system delay, expressed in milliseconds.

Signal Level	The voice signal relative level is defined as the ratio of the signal level to a 0 dBm0 reference.
Noise Level	The noise level is defined as the ratio of the silent period background noise level to a 0 dBm0 reference.
Residual Echo Return Loss	The residual echo return loss value may be measured directly by the VoIP end system's echo canceller or may be estimated by adding the echo return loss (ERL) and echo return loss enhancement (ERLE) values reported by the echo canceller.
Gmin	The gap threshold.
R Factor	The R factor is a voice quality metric describing the segment of the call that is carried over this RTP session.
External R Factor	The external R factor is a voice quality metric describing the segment of the call that is carried over a network segment external to the RTP segment
MOS Listening Quality	The estimated mean opinion score for listening quality is a voice quality metric on a scale from 1 to 5, in which 5 represents excellent and 1 represents unacceptable .
MOS Conversational Quality	The estimated mean opinion score for conversational quality defined as including the effects of delay and other effects that would affect conversational quality.
Packet Loss Concealment Algorithm	Value for this field is set to Unspecified. This means no information is available concerning the use of Packet Loss Concealment.
Adaptive Jitter buffer Algorithm	Value for this field is set to Adaptive. This means that the size is being dynamically adjusted to deal with varying levels of jitter.
Jitter Buffer Rate	This parameter is defined in terms of the approximate time taken to fully adjust to a step change in peak to peak jitter from 30 ms to 100 ms.
Nominal Jitter Buffer Size	This is the current nominal jitter buffer delay in milliseconds, which corresponds to the nominal jitter buffer delay for packets that arrive exactly on time.
Maximum Jitter Buffer Size	This is the current maximum jitter buffer delay in milliseconds which corresponds to the earliest arriving packet that would not be discarded.
Absolute Jitter Buffer Size	This is the absolute maximum delay in milliseconds that the adaptive jitter buffer can reach under worst case conditions.

Table 18 - RTCP VoIP Metric Block Parameters Supported on the UNI-V

8.2. UNI-V Voice Features Supported

This section sets out all the telephony features supported on both indoor and outdoor the UNI-V.

SIP service features	Description of feature
Call Waiting	• Accepting a second call whilst call is in progress • Alternating between two calls
Suspend Call Waiting	• Cancel Call Waiting
Call forwarding	• Hosted by the access seeker softswitch • Activation and Deactivation code configured in the Dial Plan
Call hold	• Basic hold (flash hook supported)
Hotline service	• Immediate connection to a preconfigured number
Distinctive Ringing	• Alert-info header value indicates distinctive Ringing pattern for the different distinctive Ringing features.
DTMF support	• DTMF for dialling • In band transmission • Out of Band RFC2833 transmission
Fax support	• Fax passthrough
Calling Line Identification	• Hosted by the access seeker softwsitch • Configured in the Dial Plan • Send signal to CPE to display source number of incoming call
Calling Line Identification Restriction	• Keep source number private in outbound calls • Hosted by the access seeker softwsitch • Configured in the Dial Plan
Emergency Call	• SIP Priority-headers to the access seeker's softswitch
Message Waiting Indicator	• Visual Message Waiting Indicator • Stutter Dial Tone
Voice Band Data	• Passthrough using G.711 with fixed jitter buffer size

Table 19 - Voice Features Supported on the UNI-V

8.2.1. Call Feature Triggers

This sub-section describes how various call features are triggered.

8.2.1.1. Call Waiting

Call Waiting: If the UNI-V has Call Waiting enabled and access seeker's softswitch allows more than one call to the UNI-V, then Call Waiting will be triggered when a second call is received by the UNI-V. The call hold feature is not required for the call waiting feature to be triggered.

If an End User has Call Waiting enabled on the UNI-V and call forwarding (both busy and no answer) is activated on access seeker's softswitch, when the UNI-V receives a second call, the following features will be triggered depending on the softswitch call forwarding timers:

- If access seeker's softswitch call forwarding no answer timer is less than the Call Waiting timeout of the UNI-V (UNI-V Call Waiting timeout is 60 seconds), call forwarding no answer is triggered by the softswitch.
- If access seeker's softswitch call forwarding no answer timer is greater than the Call Waiting timeout of the UNI-V (UNI-V Call Waiting timeout is 60 seconds), the UNI-V will generate "486 Busy", triggering the call forward busy logic on access seekers' softswitch.

The UNI-V Call Waiting feature is configured in the TR-104 "CallWaitingEnable" parameter under the VoiceProfile.{i}.Line.{i}. CallingFeatures object.

UNI-V Call Waiting is dependent on access seeker's softswitch allowing two or more simultaneous calls to be made the same UNI-V.

The UNI-V supports the Call Waiting Tone specified in AS/CA S002:2010. The frequencies, amplitudes, and timing are specified in the UNI-V Electrical Specification documentation.

Call Waiting occurs when an INVITE for a new dialog is received during an active call. When Call Waiting is invoked, the UNI-V immediately sends "486 Busy" responses to subsequent INVITES (only one call can be waiting).

When an End User is in a conversation and receives a Call Waiting Tone, indicating an additional incoming call, the End User can:

- Ignore the 2nd call;
- Accept the 2nd call; or
- Toggle between the two calls (after accepting the 2nd call).

The UNI-V starts a 60 second Call Waiting timer when the Call Waiting signal is received, and the timer is cancelled when the Call Waiting call is answered or cancelled. If the timer expires (Call Waiting call ignored) the UNI-V sends a "486 Busy" response to access seeker's softswitch.

If access seeker's softswitch applies its own no-answer or Call Waiting service in parallel with the UNI-V's Call Waiting service, access seeker's softswitch can abort the unanswered Call Waiting call by sending a "CANCEL" message as per normal RFC3261 signalling.

Table 20 describes the UNI-V Call Waiting service codes.

Service Code	Description
Recall	The active call is held and a dial tone is generated
Recall + digit 1	The active call is released and the held call is resumed.
Recall + digit 2	The active call is held and the incoming call waiting call is accepted, or The active call is held and the held call is resumed

Table 20 - Call Waiting service codes

Call Waiting can be separated into two stages, before and after accepting the second incoming call as described in the following sub-sections. For illustrative purposes, it is assumed that A and B are on an established the call when C calls A, invoking Call Waiting.

8.2.1.1.1. Before accepting the second incoming call

When C calls A, A receives Call Waiting Tone and C hears the Ring Back Tone.

If A presses Recall, B is placed on hold by sending a re-INVITE, and A hears Dial Tone.
Then:

Service Code *(action by user A)*	Description
digit '2'	• A accepts the call from C (B is on hold).
Recall pressed again	• A continues to hear dial-tone. C continues to hear ring back tone. The call with B is released and the call from C is rejected after timeout (12 sec).
Timeout	• A does not press a valid digit key before dial tone timeout (12sec). • A hears busy tone. • The call with B is released and the call from C is rejected.
A goes on hook	• The call with B is released and A is rung for the call from C. Note if A is the called party of the A-B call a 90s release guard period is applied which is greater than the Call Waiting time out period.
Any other digit	• Ignored

Table 21 - Call Waiting - Before accepting the second incoming call

8.2.1.1.2. After accepting the second incoming call

Assuming the active call is A-C and the held call is A-B, when A presses the Recall key, the active call is placed on hold and A hears dial tone (both calls are now on hold).

Then:

Service Code *(action by user A)*	Description
digit '1'	• the active call (A-C) is released and the held call (A-B) is resumed.
digit '2'	• the active call (A-C) remains on hold (held when recall key pressed) and the held call (A-B) is resumed (toggles between active and held calls).
Recall pressed again	• the active call (A-C) is resumed and the held call (A-B) remains held.
A goes on hook	• the active call (A-C) is released and A is re-rung by the held call (A-B). • If A is the called party of the active call (A-C) a 90s release guard period is applied. A can either pick up the phone to resume the held call or wait for ringing timeout (60s) to release the call.
Timeout (12 sec)	• A does not press any valid digit before dial tone timeout (12s), A will hear busy tone and both calls are released.
Invalid Entry	• If A does not press any valid digit key before dial tone timeout (12s), A will hear busy tone and both calls are released. e.g. digits '0' or '4'…'9'

Table 22 - Call Waiting - After accepting the second incoming call

8.2.1.2. Suspend Call Waiting

Call Waiting can be suspended for a single call by the End User dialling the UNI-V's "Suspend Call Waiting" feature code *70 (fixed value). After dialling *70, the Dial Tone is played.
Call Waiting can be suspended for either:

- New calls – by dialling *70 before the called number, for example dial *70<dial-tone> 12345678.
- Existing call – by pressing Recall, dialling *70 then pressing Recall again (resumes active call), i.e., by following the sequence, Recall <dial-tone> dial *70 <dial-tone> Recall.

Call Waiting is re-activated at the end of the call.

To use "Suspend Call Waiting", the digit map must contain a pattern that matches or partially matches *70, e.g. *X.T.

8.2.1.3. Call Forwarding

Call forwarding on busy, Call forwarding on no answer, and unconditional call forwarding are controlled by access seeker's softswitch. To activate/deactivate call forwarding, the Dial Plan on the UNI-V must be configured with the same activation and deactivation dial codes implemented at access seeker's softswitch.

Call forwarding (on busy, no answer or unconditional) is not a UNI-V feature, but rather a function of access seeker's softswitch. Specifically, the UNI-V does not support:

- Splash ring / ping ring; or
- A special Dial Tone when call forwarding is active.

8.2.1.4. Call Hold

The End User can initiate call hold during an existing call session. Subsequent actions are that:

- the End User recovers the original callthe End User initiates a second call, then
- the second call is either held or released and returned to the first call

Table 23 describes the service codes supported by the UNI-V.

Service Code	Description
Recall	The current call is held and a Dial Tone is generated
Recall + digit 1	The current call is released and the held call is resumed
Recall + digit 2	The current call is held and the held call is resumed

Table 23 - Voice Features supported on the UNI-V

Call hold can be separated into 2 stages, before and after the second call is established as described in the following sub-sections. For illustrative purposes, it is assumed that A and B are on an established call when A invokes Call hold using the Recall key. B is placed on hold by sending a SIP re-INVITE and A hears dial tone.

8.2.1.4.1. Before second call is established

When A presses Recall, B is placed on hold through the UNI-V sending a re-INVITE, and A hears the Dial Tone.

Service Code *(action by user A)*	Description
Recall (pressed again)	• User A is reconnected with B.
2nd number dialled (e.g. C party)	• If the call to user C is successful, A can communicate with C *(see table below for subsequent operation)* o 2nd number can be a service activation code or another phone number. • If A presses Recall key before the call to C is accepted or rejected, the call to C is released and A is reconnected with B. • If the call to C is rejected, A hears busy tone. o If A presses Recall key, A is reconnected with B o If A goes on-hook, A is alerted by ringing (re-rung) to indicate that B is still held. A can then pick up the phone to be reconnected with B.
Timeout (12 sec) – no user input	• If A does not dial any digit before dial tone timeout (12 sec), A hears busy tone o If A then presses the Recall key A is reconnected with B. o If busy tone times out (60s) the call with B is released and A hears Howler tone.
A goes on-hook (prior to timeout)	• If A goes on-hook a local ringback occurs and the call with B may be picked up.

Table 24 - Call Hold - Before second call is established

8.2.1.4.2. After second call is established

Following the scenario in previous section, after the call to C is accepted, if A presses Recall, A hears dial tone. The following actions may occur:

Service Code *(action by user A)*	Description
Recall (pressed again)	• A presses Recall key, the active call (A-C) is resumed and the held call (A-B) remains held.
Digit '1'	• the active call (A-C) is released and the held call (A-B) is resumed.
Digit '2'	• the active call (A-C) remains on hold (held when recall key pressed) and the held call (A-B) is resumed (toggles between active and held calls).
A goes on hook	• The active call (A-C) is released and A is alerted by ringing (re-rung) to indicate a call is still held (i.e. A-B). • A can either pick up the phone to resume the held call or wait for ringing timeout (60s) to release the call.
Timeout (12 sec)	• A does not press any valid digit key before dial tone timeout (12s), A will hear busy tone o If A presses Recall key the active call (A-C) is resumed and the held call (A-B) remains held. If busy tone times out (60s) the calls with B and C are released and A hears Howler tone.

Table 25 - Call Hold - After second call is established

8.2.1.5. Hotline Service

The UNI-V's hotline (immediate) service is self-contained and does not rely on any softswitch hotline capability.

The hotline destination is pre-provisioned using the TR-104 "X_ALCALTE-LUCENT-COM_DirectConnectURI" parameter under the VoiceProfile.{i}.Line.{i}. CallingFeatures object.

At off-hook detection, the UNI-V does not play the Dial tone and immediately sends an INVITE request with the FROM header populated with the value of the X_ALCALTE-LUCENT-COM_DirectConnectURI field.

Once the INVITE has been sent, normal call processing is applied between the UNI-V and softswitch.

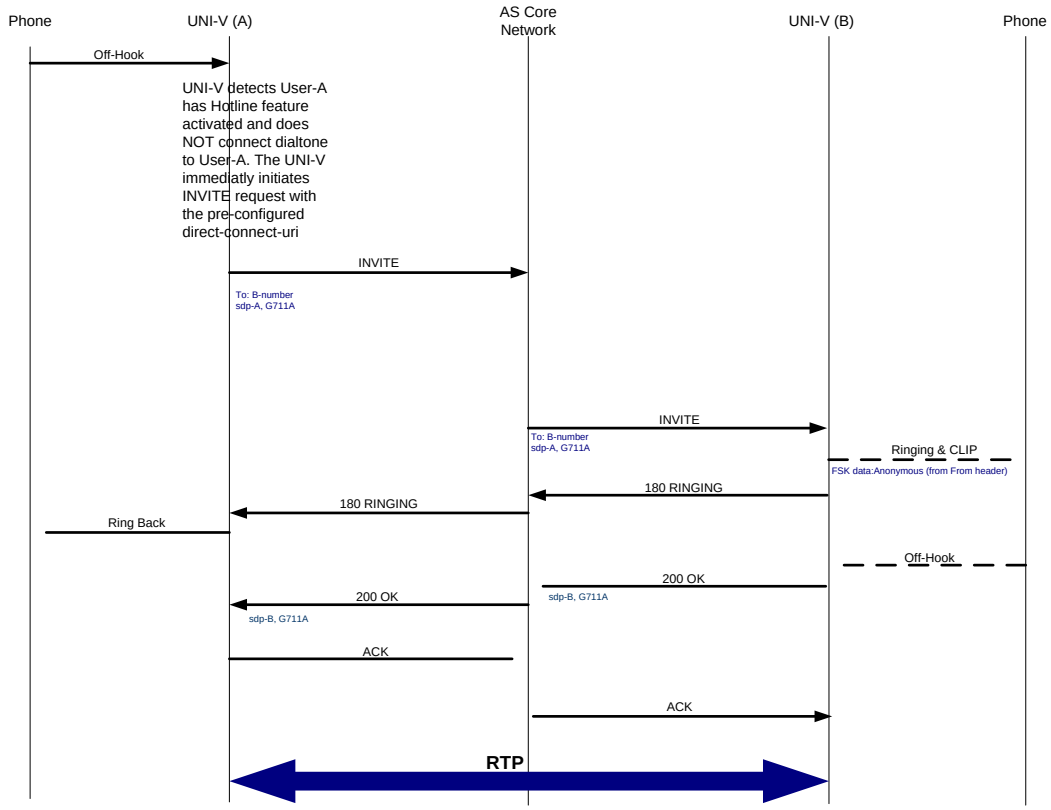


Figure 7 - Hotline SIP Flow

8.2.1.6. Distinctive Ringing Support

The UNI-V supports 5 different Ring cadences (DR0, DR1, DR3, DR6 and DR7) with timings defined in AS/CA S002:2010. When an INVITE is received by the UNI-V for a new call, the UNI-V will act as follows depending on the value in the INVITE "alert-info" header:

- If the "alert-info" value is in one of the UNI-V supported formats:

  <http://127.0.0.1/*[anytext]*/dst_ring_*[ring-cadence-index]*>

  <http://127.0.0.1/*[anytext]*dr*[ring-cadence-index]*>

  Note the underscore character between "dst" and "ring" and between "ring" and the ring cadence number.

  Then the *[ring-cadence-index]* value determines the distinctive Ringing pattern in accordance with Table 26:

Ring-cadence-index value	Distinctive Ringing pattern
1	DR0
2	DR1
3	DR3
4	DR6
5	DR7

Table 26 - Distinctive Ring Cadences

- If the "alert-info" header is not presented, the default cadence (DR0) will be applied.
- If the "alert-info" header contains an invalid value, the default cadence (DR0) will be applied.

The UNI-V does not include an "alert-info" header in outgoing SIP INVITE requests.

8.2.1.7. DTMF Support

DTMF Tones will be encoded as normal voice data (in-band) or using RFC2833.

When in-band DTMF is configured, DTMF is transmitted within the audio of the phone conversation (i.e. it is audible to the conversation partners). Only an uncompressed codec (G.711 A-law) can carry in-band DTMF reliably.

When RFC2833 is configured, DTMF tones are encoded in RFC2833 packets and there must be SDP negotiation and agreement by both ends of the bearer channel to allow its use. This negotiation follows standard offer/answer rules in RFC3264. The NTD will offer RFC2833 or include it in an SDP answer only if the RFC2833 parameter is enabled in the TR-104 configuration. The "telephone event" format contains a MIME registration with media type "audio" and media subtype "telephone-event". The DTMF will be signalled in the SDP "a=rtpmap" line and a dynamic RTP payload type of 97.

Note that during SIP signalling offer/answer, if the other party to the call does not support RFC2833, the UNI-V (with RFC2833 configured) will revert back to In-Band carriage of DTMF using G.711.

DTMF using in-band or RFC2833 is controlled by the UNI-V and is configured in TR-104 "DTMFMethod" under VoiceProfile.{i} object.

8.2.1.8. DTMF Assurance

The UNI-V supports both in-band and out-of-band DTMF to cater for an access seeker's preferred telephony network topology.

The RFC2833 out-of-band DTMF method is offered to customers subject to the provisions outlined in section 6.8 (Industry Process for detection of false DTMF signalling) of the Comms Alliance G646:2012, *Wholesale Services Definition Framework – Telephony Access Service*.

8.2.1.9. Decadic support

Decadic or pulse dialers are not supported by the UNI-V.

8.2.1.10. FAX Support

The UNI-V can support the transmission of fax across the NBN Co Network:

Fax pass-through is only supported with the G.711 A-law codec. This is the default setting. Fax is encoded in G.711 A-law similar to voice traffic. Once a SIP call is setup, the UNI-V will automatically switch the codec to clear channel (G.711 A-law codec with jitter buffer fixed and echo cancellation disabled). Data will be sent using the same packetisation delay as other UNI-V telephony traffic (i.e. 20ms).

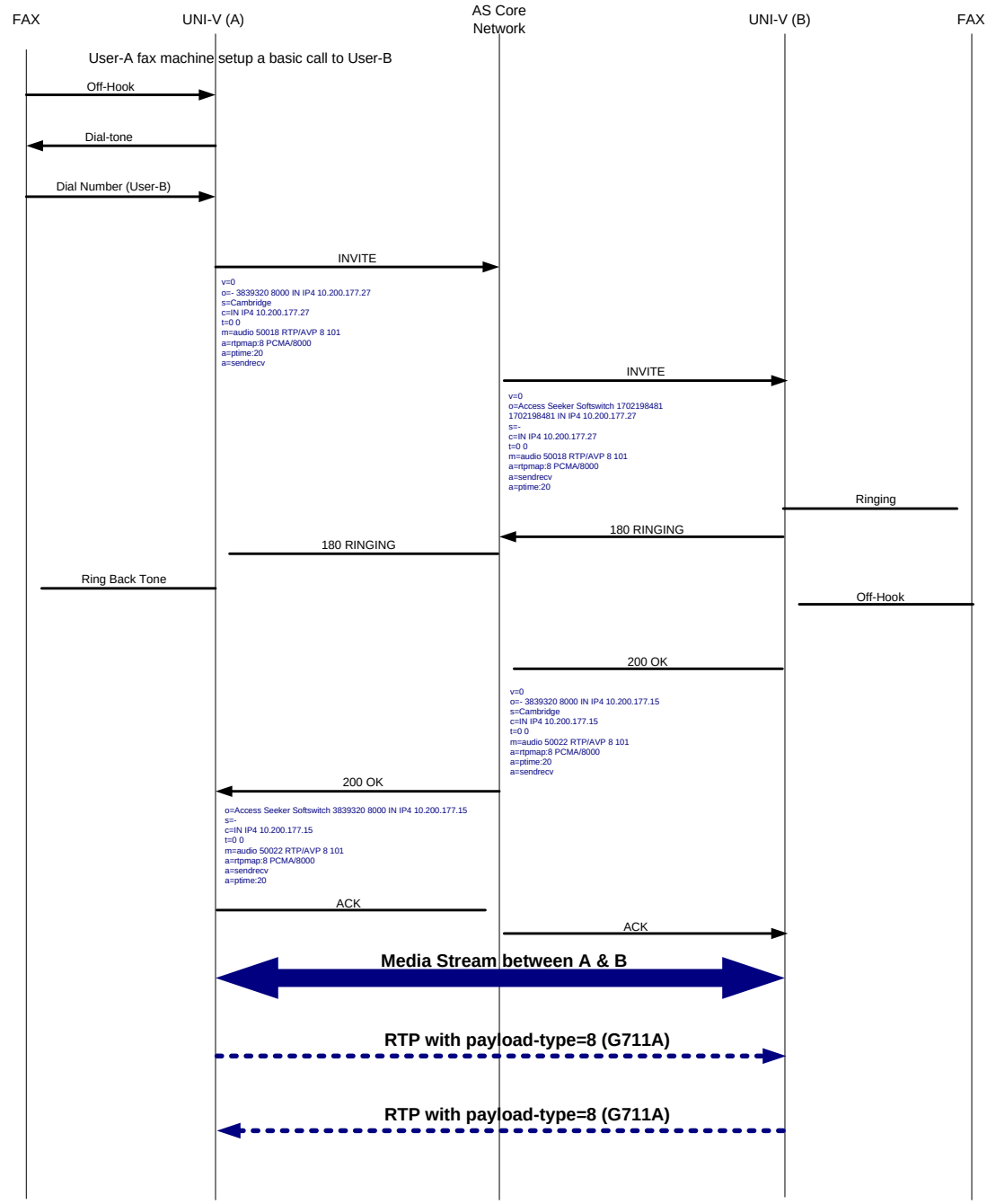


Figure 8 - Fax Pass-Through

8.2.1.11. Calling Line Identification

Calling Number Display (**CND**) is implemented in the following states:

- During On-Hook
- Phone Off-Hook (when a second call is received using Call Waiting feature).

When a SIP INVITE message is received at the UNI-V, the UNI-V utilises the "P-Asserted-Id" header or if it is not present the "From" header. The CND feature is controlled by the UNI-V and is configured in the TR-104 "CallerIDEnable" parameter under the VoiceProfile.{i}.Line.{i}. CallingFeatures object.

When CallerIDEnable is set to "true", FSK is then used to output the caller ID to the CPE connected to the UNI-V. If however CallerIDEnable is set to "false", no caller ID will be sent to the CPE.

Access seeker can still control CND through its softswitch when enabled on the UNI-V by setting the softswitch to not include P-Asserted-Id in the SIP INVITE messages and setting the "From" Header to anonymous.

8.2.1.12. Calling Line Identification Restriction

Calling Line ID Restriction (**CLIR**) is not a UNI-V feature, but rather a function of access seeker's softswitch.

CLIR is normally implemented by access seeker's softswitch using a prefix sequence before the dialled number (e.g. *67 followed by the required number to dial). The CLIR prefix must be considered when configuring the Dial Plan (digit map).

8.2.1.13. Message Waiting Indication

The Message Waiting Indication feature allows the UNI-V End User to be notified (RFC3842) when they have a message waiting in their message service. The UNI-V supports implicit message waiting subscription (it does not send a message waiting subscribe message).

Access seeker's network must send a SIP NOTIFY message with "Messages-Waiting" header set to "yes" and "Voice-Message" set to the "n" number of messages whenever the message count changes and when the UNI-V completes registration unless the message count is zero.

When the SIP NOTIFY "Messages-Waiting" header is set to "yes", Visual Message Waiting and Audible Message Waiting are activated as follows:

1) Visual Message Waiting: the UNI-V will send FSK signals that causes a blinking led on the CPE connected to the UNI-V where supported.
2) Audible Message Waiting: the UNI-V plays Message Wait Tone (Stutter Dial Tone) instead of standard Dial Tone when the UNI-V user goes off-hook.

When the SIP NOTIFY "Messages-Waiting" header is set to "no", Visual Message Waiting and Audible Message Waiting are de-activated.

The MWI feature is controlled by the UNI-V and is configured in the TR-104 "MWIEnable" parameter under the VoiceProfile.{i}.Line.{i}. CallingFeatures object.

8.2.1.14. Emergency Call

If access seeker suffixes emergency numbers with “E” within its Dial Plan (eg. “000E” and “106E”), the UNI-V will support special call handling when an emergency call is originated by the End User (subject to, among other things, mains or battery power being supplied to the NTD).

The initial INVITE message will contain two priority headers:

- Priority: emergency
- Resource-Priority: emrg.0

The UNI-V provides an emergency call treatment only for outgoing calls. When an emergency call is initiated, the emergency attributes comes into effect only after an emergency call gets answered.

During an emergency call, the UNI-V will ignore flash-hook (e.g. call hold etc) and any new incoming call is denied with “486 Busy Here”.

Note that digit map entries, when used with the “E” suffix, should define an exact match with emergency destination numbers, e.g. “000E”. Use of other digit map operators such as “x”, “.” and “T” for further digit analysis is not supported in conjunction with emergency calls.

9. SIP Flows/Call Scenarios

9.1. Authentication

A 401 or 407 response to a request from the UNI-V may contain information that the UNI-V can use to authenticate the UNI-V according to the rules in RFC3261. The UNI-V will re-send the request with updated information based on configured username, and password parameters described in the SIP configuration section. Authentication is supported for REGISTER and INVITE messages.

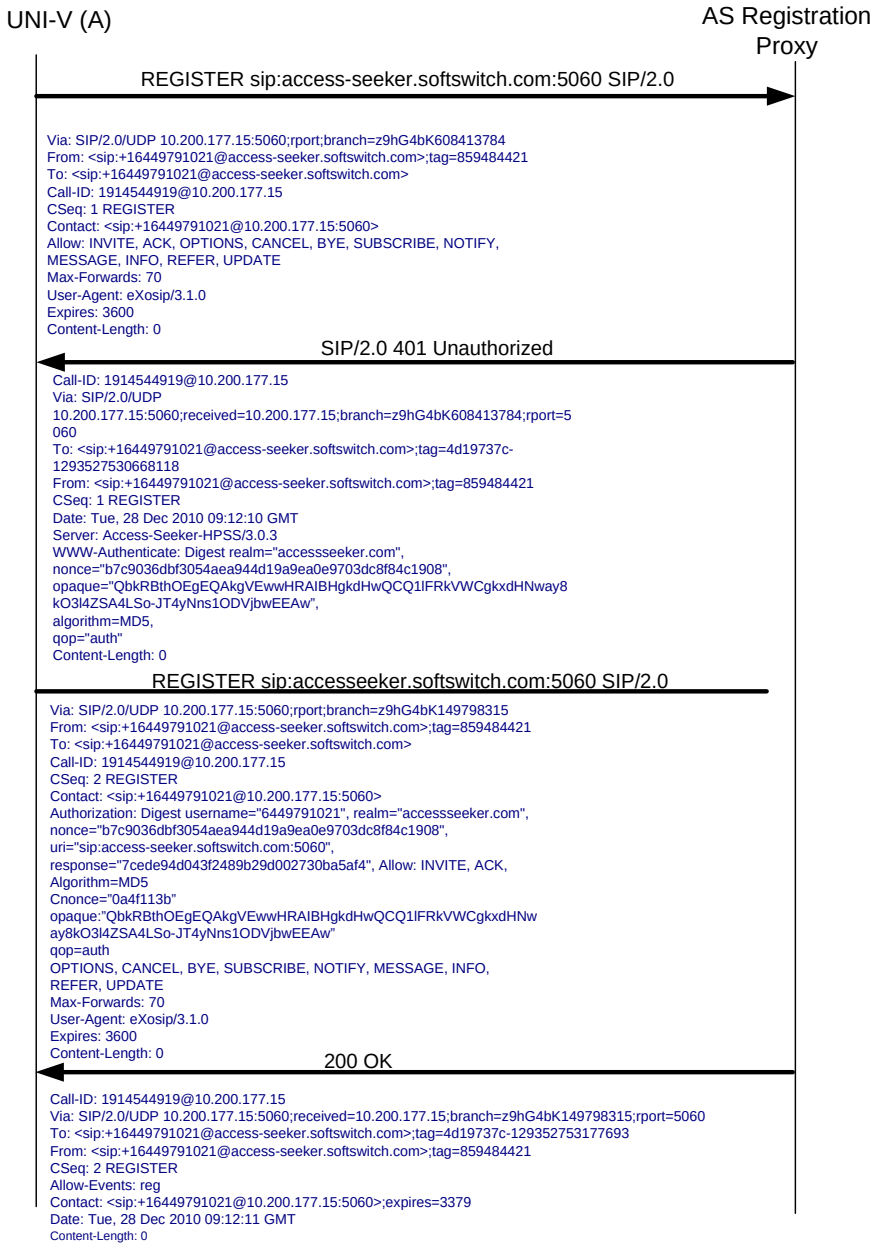


Figure 9 - SIP Registration and Authentication

9.2. Registration Failure- Incorrect Password

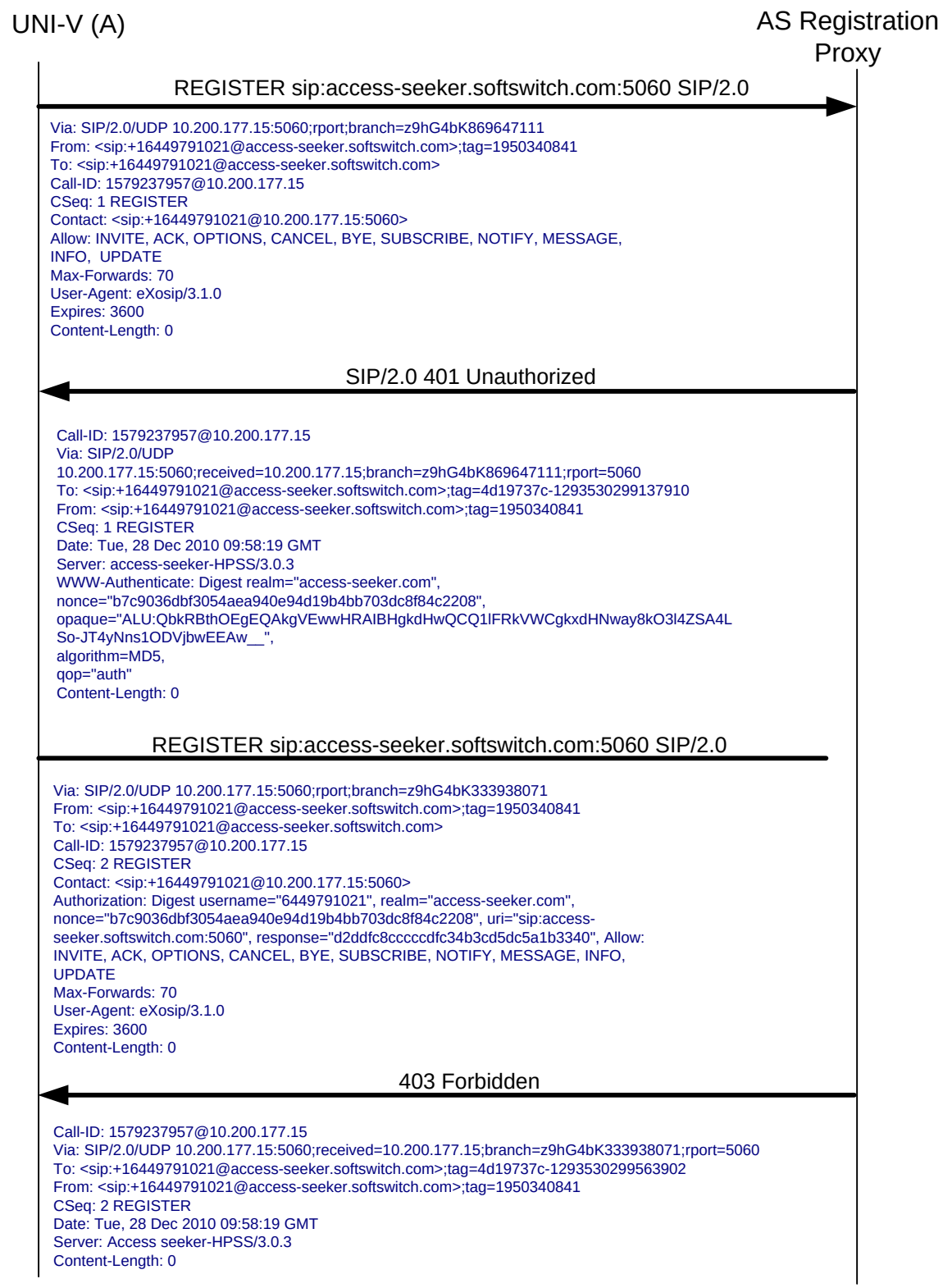


Figure 10 - Registration Failure - Incorrect Password

9.3. Registration Failure- Invalid Number

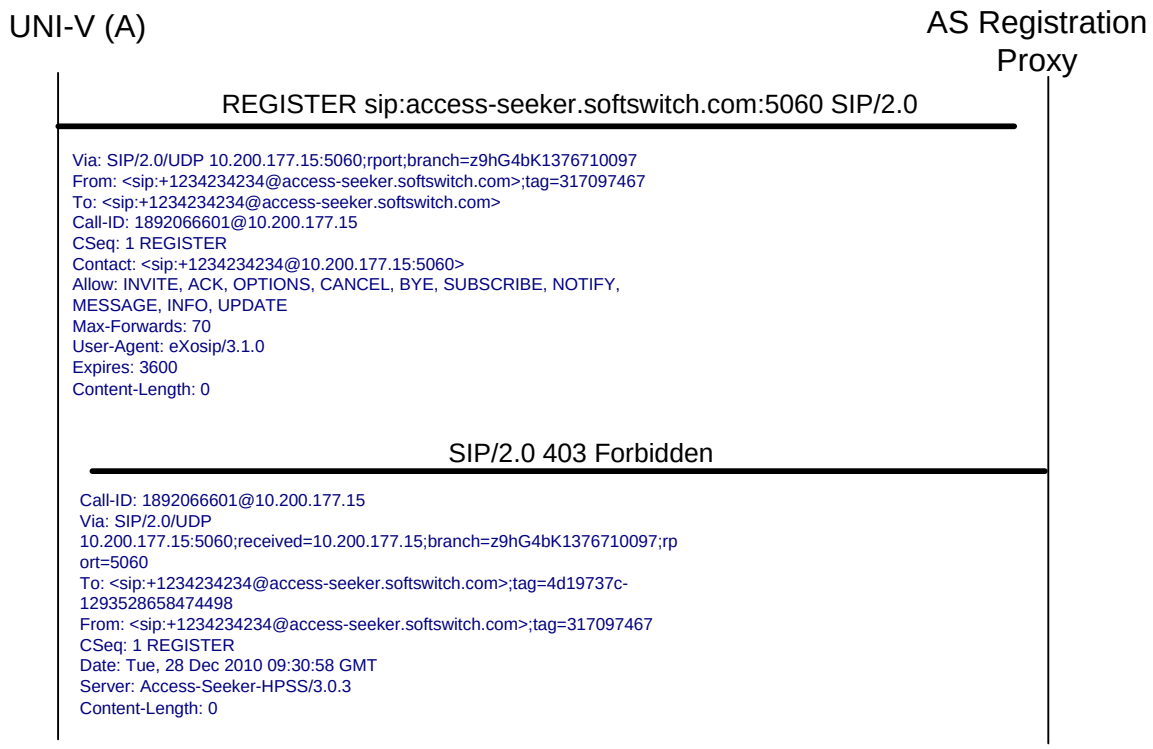
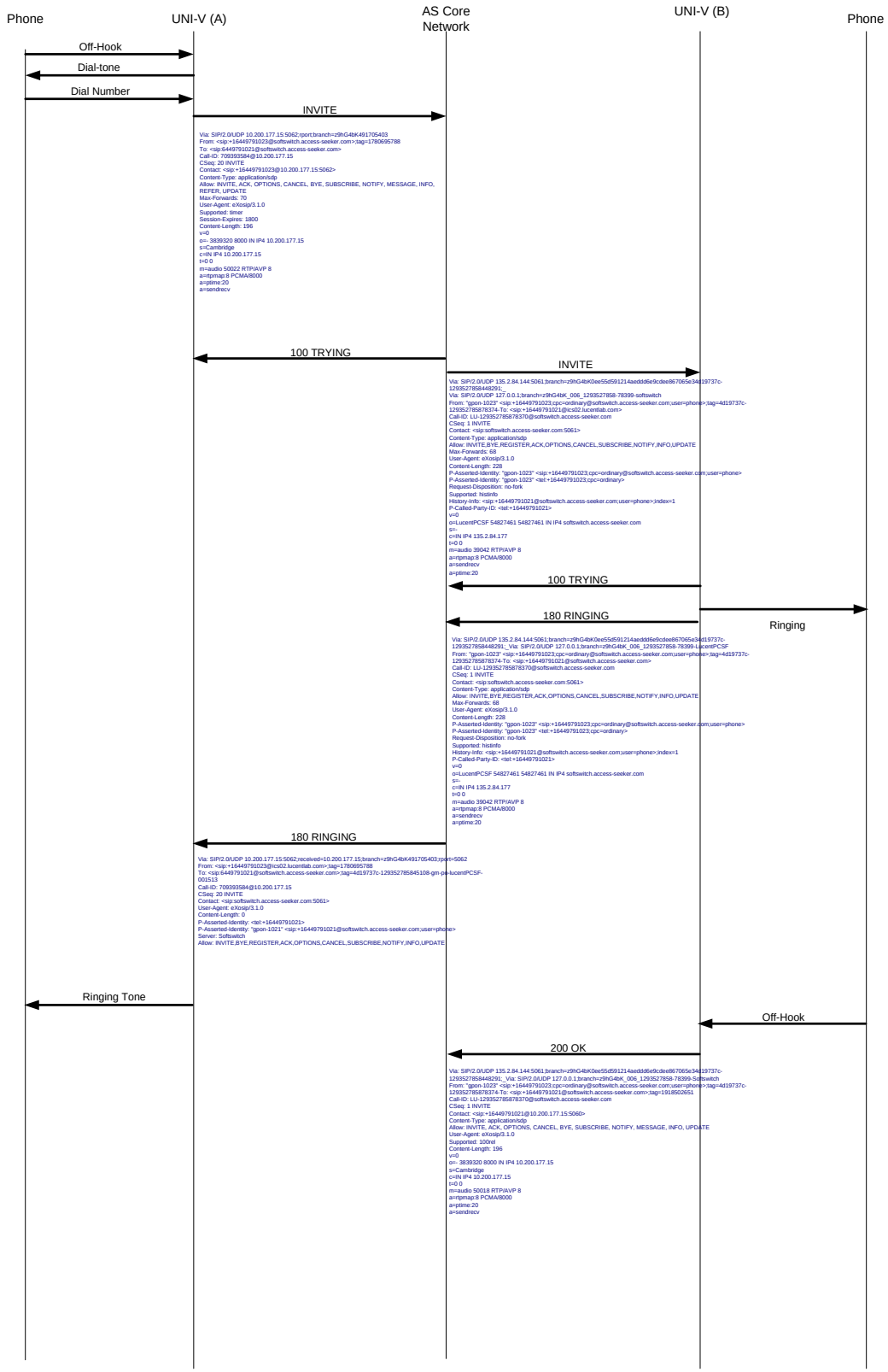
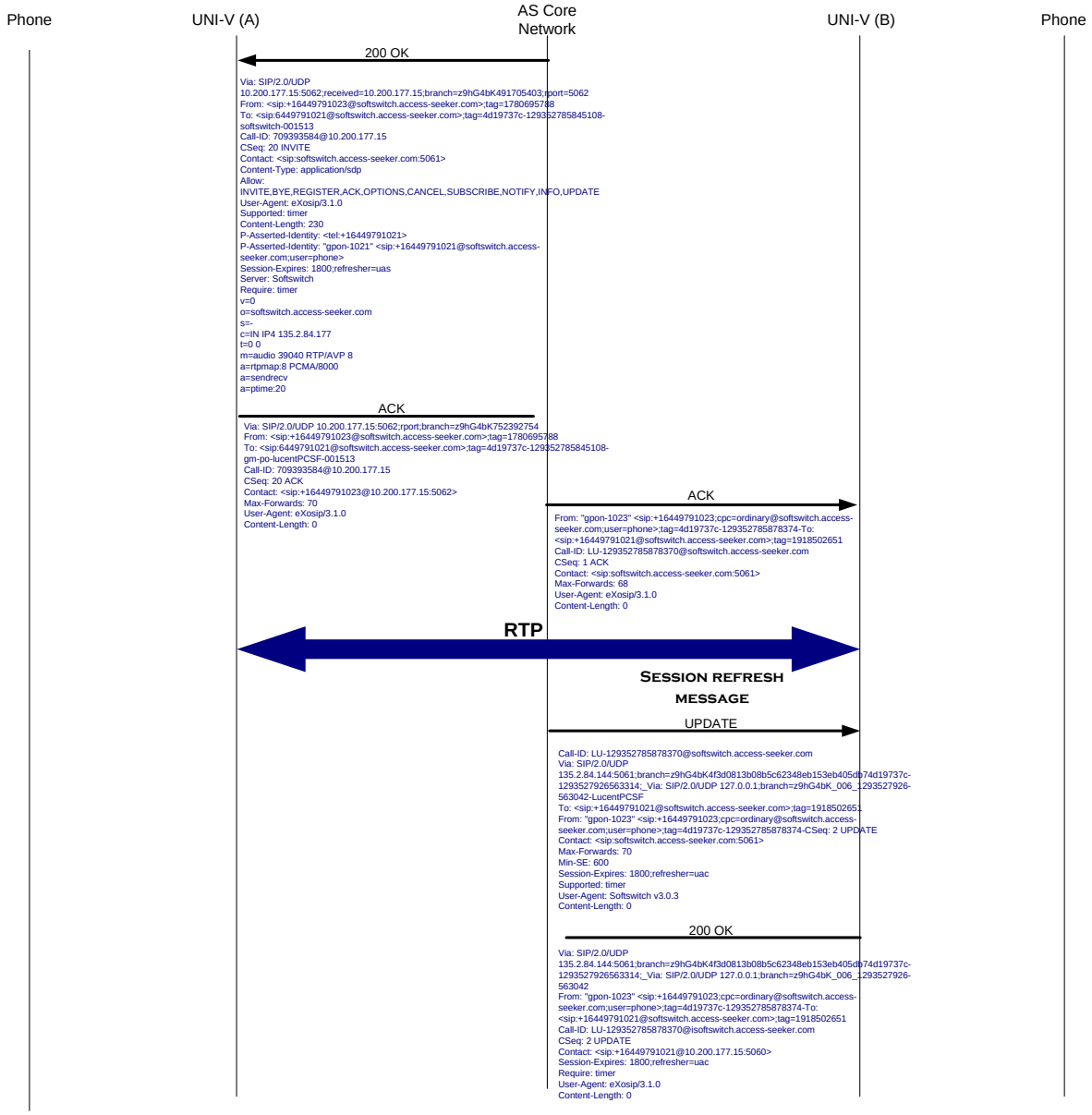


Figure 11 - Registration Failure - Invalid Number

9.4. Basic Call





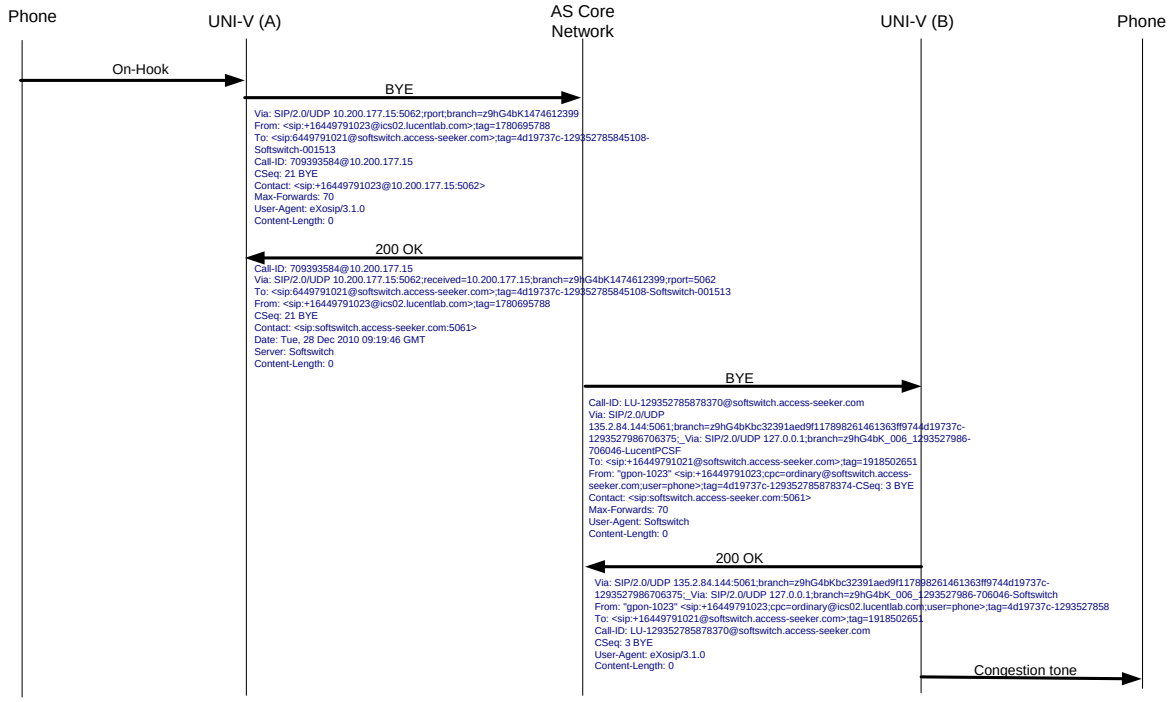


Figure 12 - SIP Signalling Basic Call Flow

9.4.1. Basic Call (No Answer)

In a basic call scenario, when UNI-V (A) calls UNI-V (B), UNI-V (B) will terminate the call (if no answer) after 60 seconds by sending a "408 Request timeout" as shown in the below diagram:

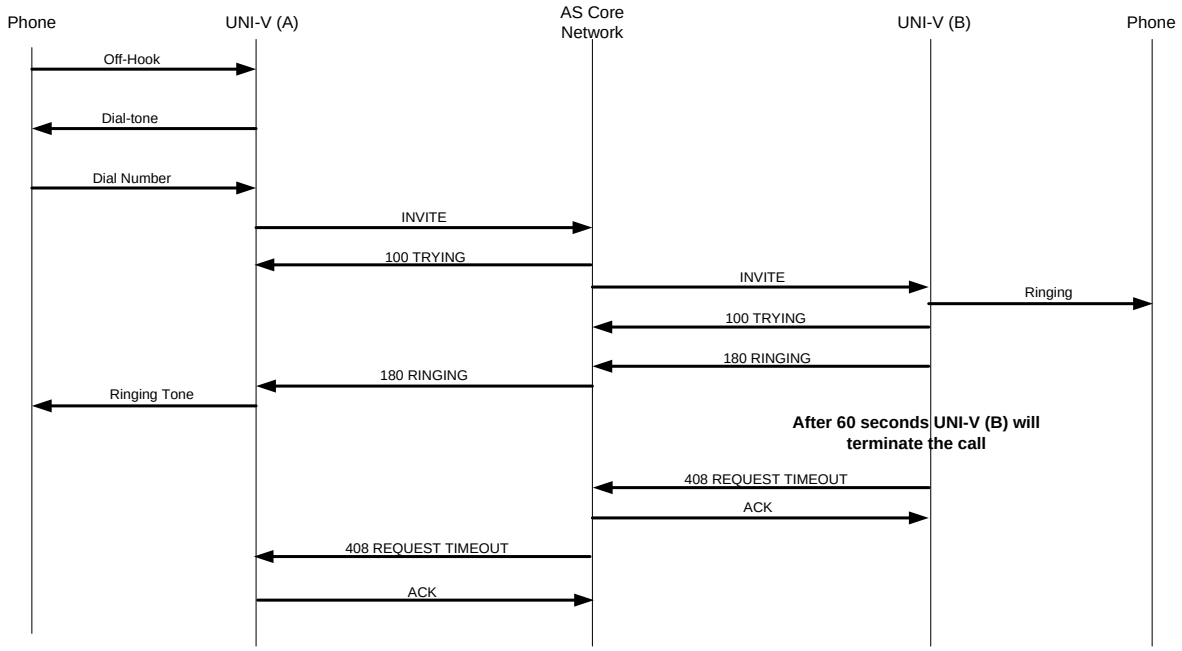


Figure 13 - Basic Call (No Answer)

9.5. Call Forwarding on Busy

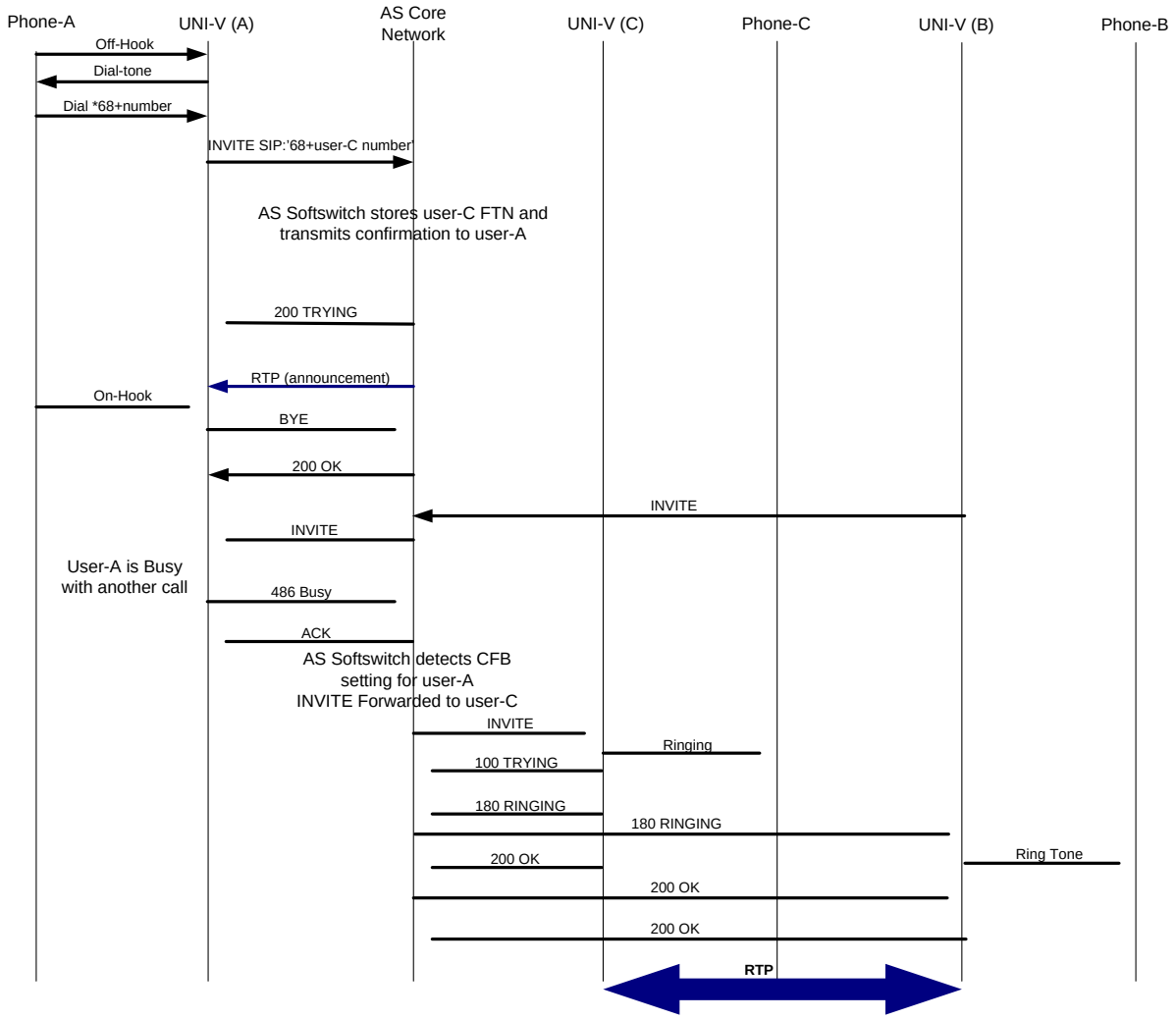


Figure 14 - Call Forwarding on Busy SIP Flow

9.6. Call Forwarding on No Answer

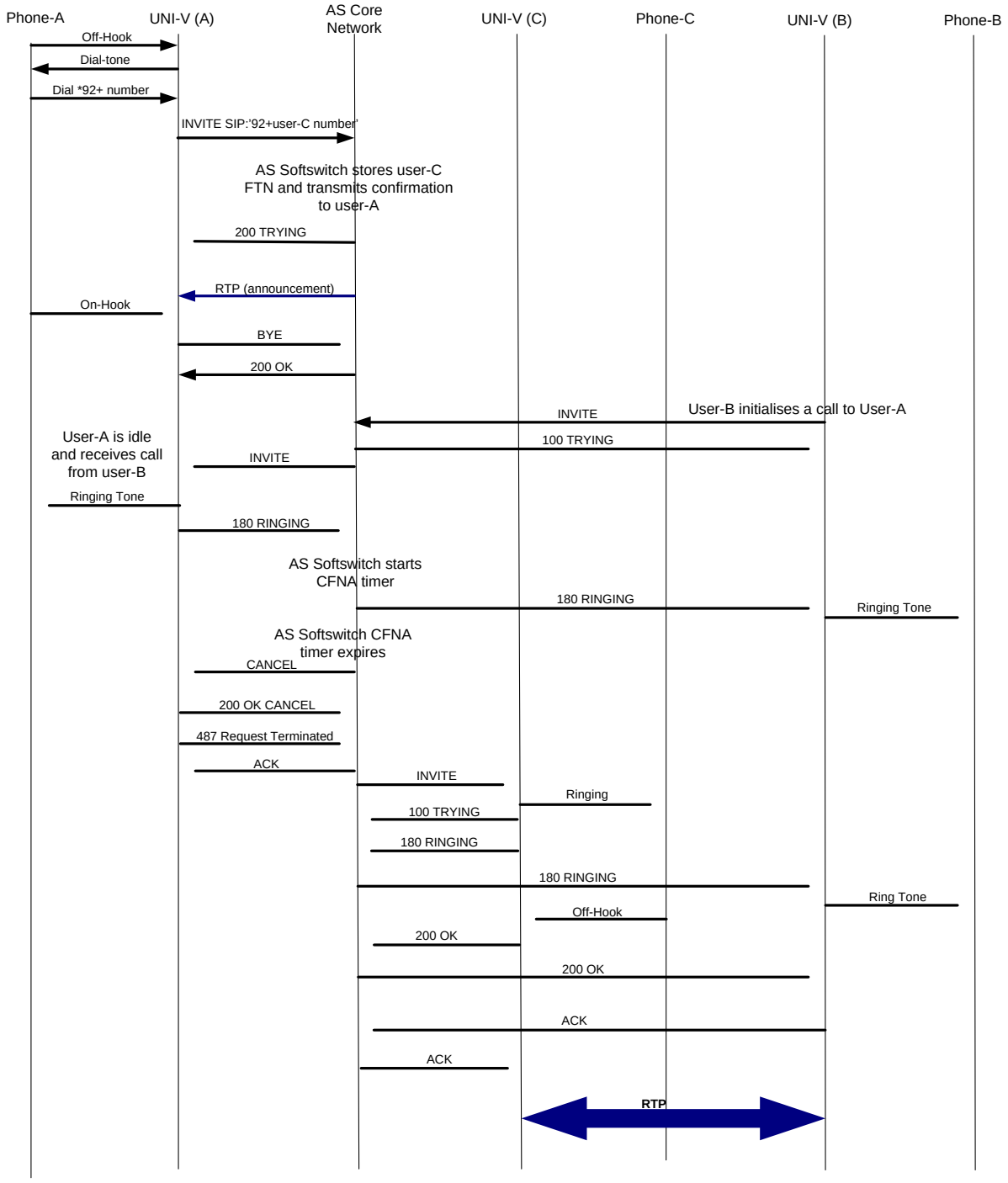


Figure 15 - Call Forwarding SIP flow - No Answer

9.7. Call Forwarding (Unconditional)

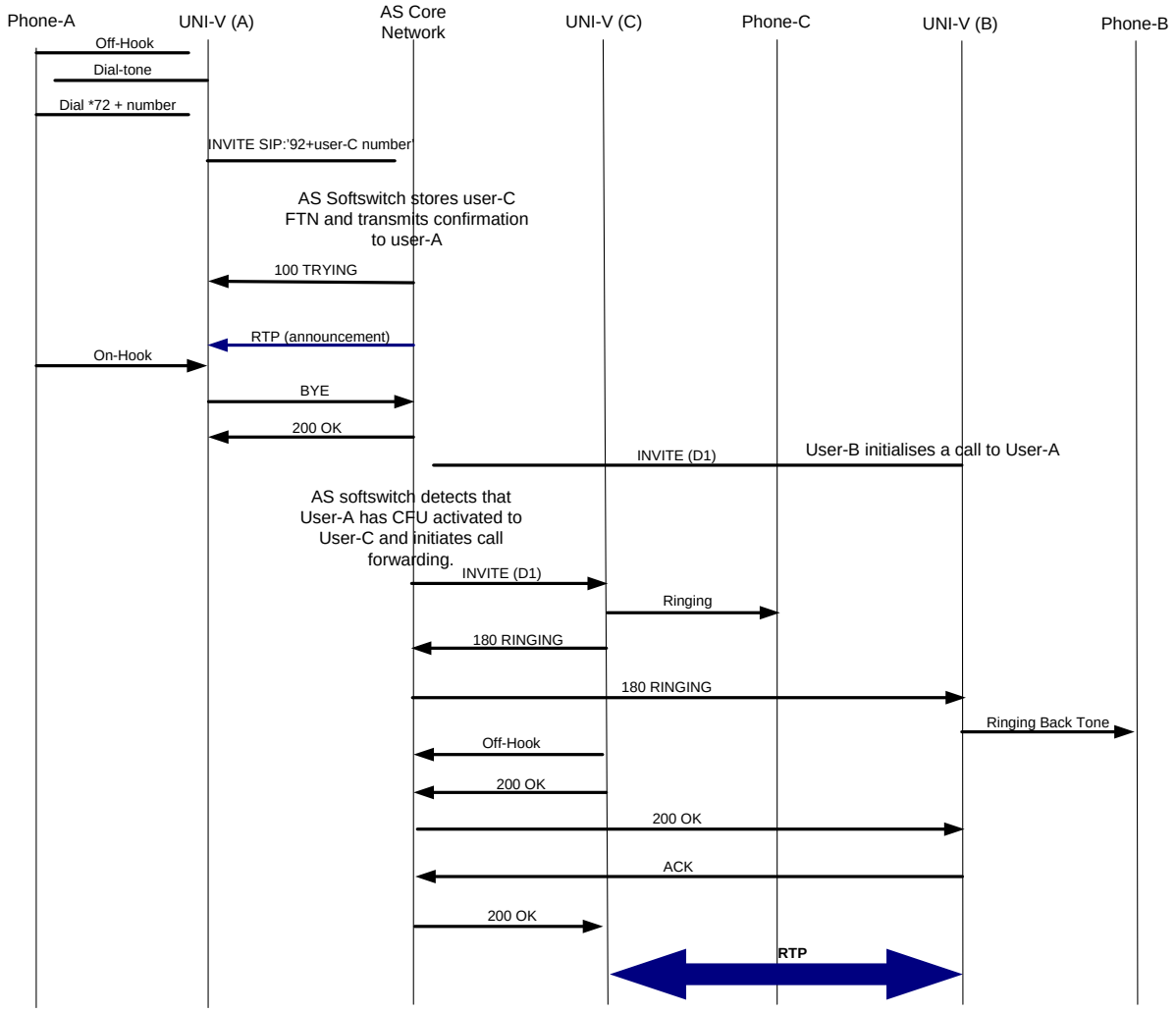


Figure 16 - Call Forwarding SIP Flow - Unconditional

9.8. Call Hold

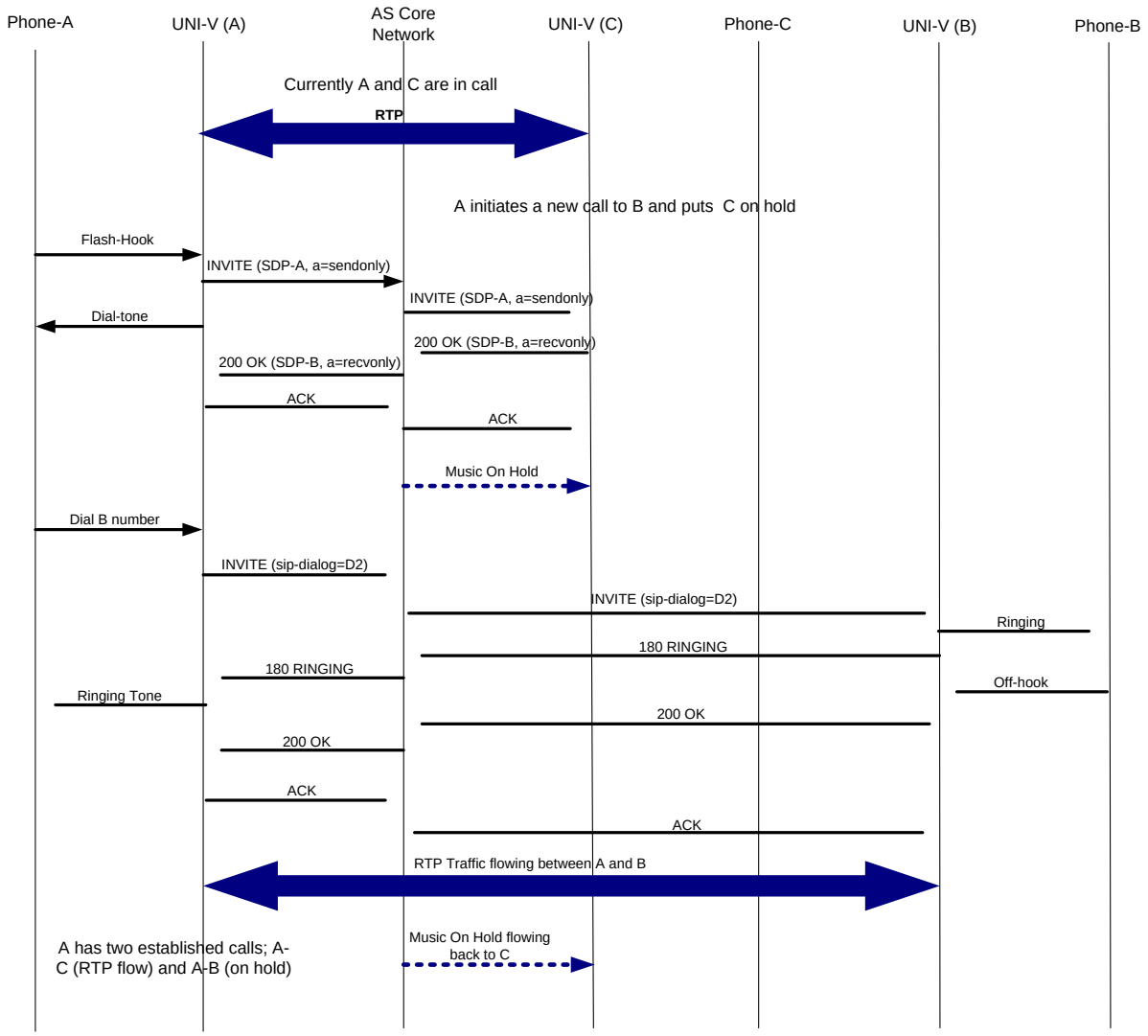


Figure 17 - Call Hold SIP Flow

9.8.1. Caller Resumes the Held Call

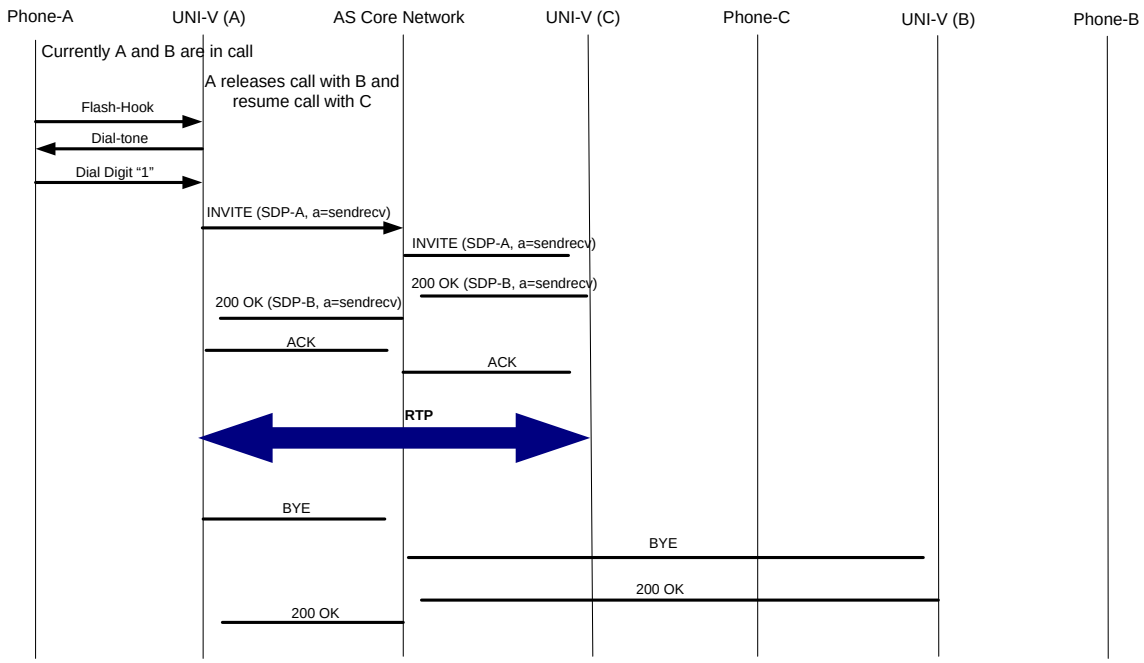


Figure 18 - Caller Resumes the Held Call

9.9. Call Waiting

9.9.1. Call Waiting received- Ignore 2nd Call (softswitch Call Waiting timer triggered)

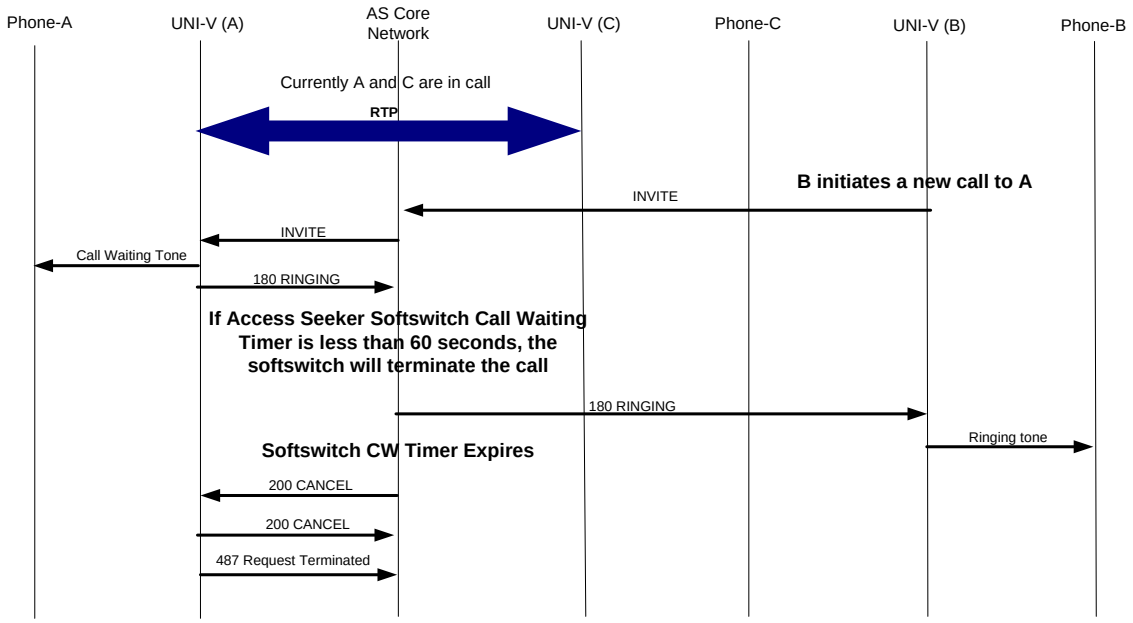


Figure 19 - Call Waiting - Ignored Second Call: softswitch Call Waiting timer triggered

9.9.2. Call Waiting received- Ignore 2nd Call (UNI-V Call Waiting timer triggered)

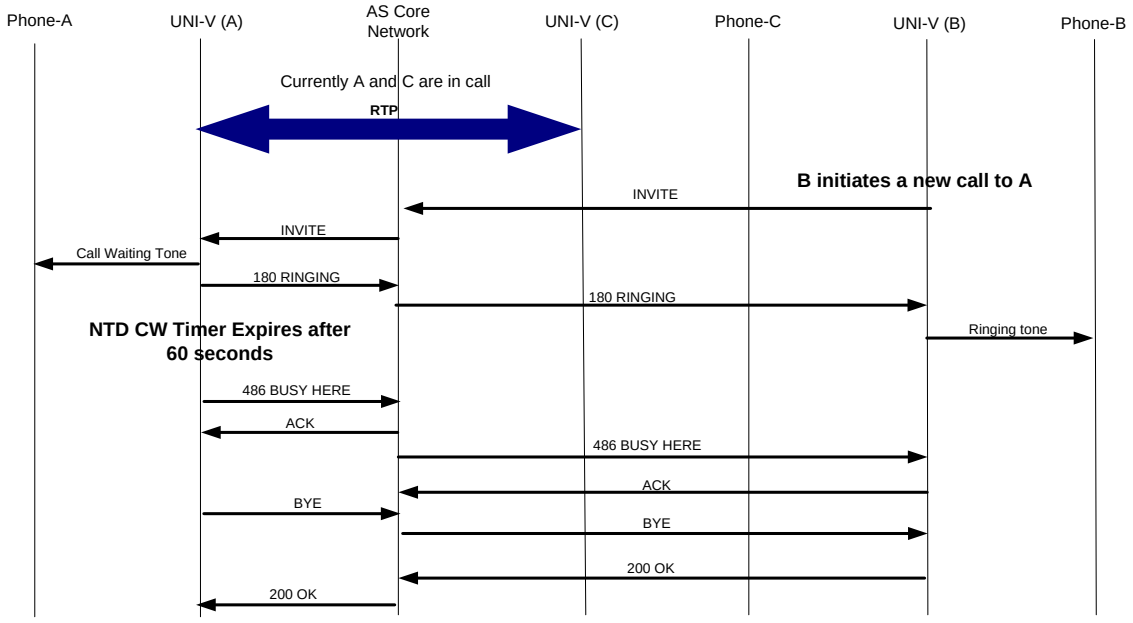


Figure 20 - Call Waiting - Ignored Second Call: UNI-V Call Waiting timer triggered

9.9.3. Call Waiting Received- Accept 2nd Call

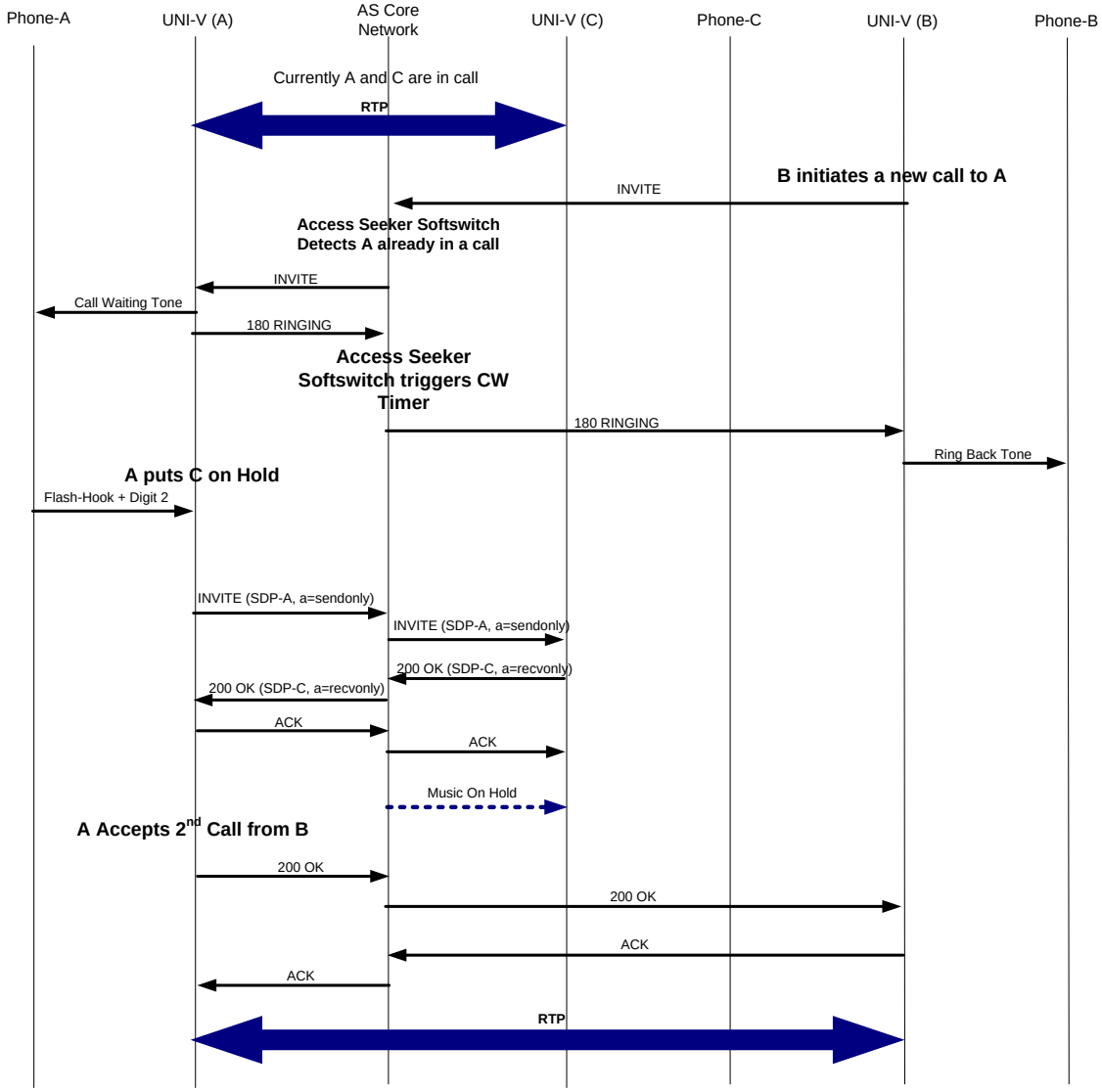


Figure 21 - Call Waiting Received - Accept Second Call

9.9.4. Call Waiting Received- Resumes Held Call

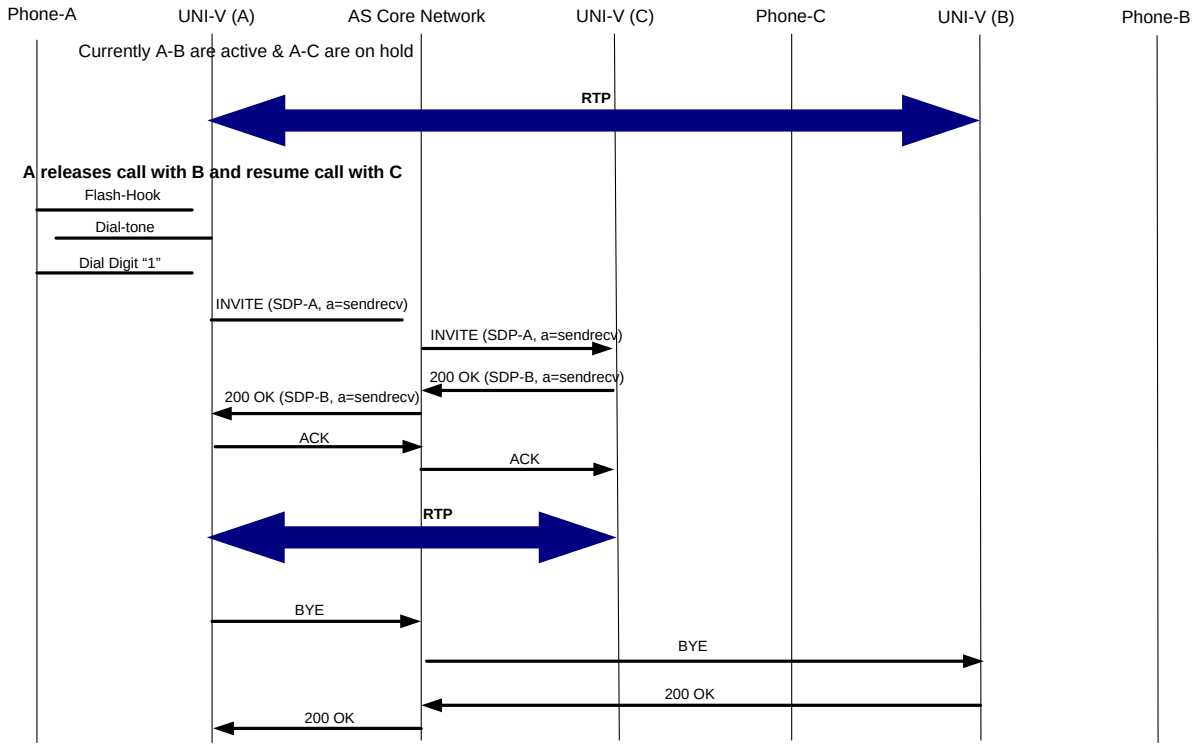


Figure 22 - Call Waiting Received - Releases Second Call

9.10. Distinctive Ringing

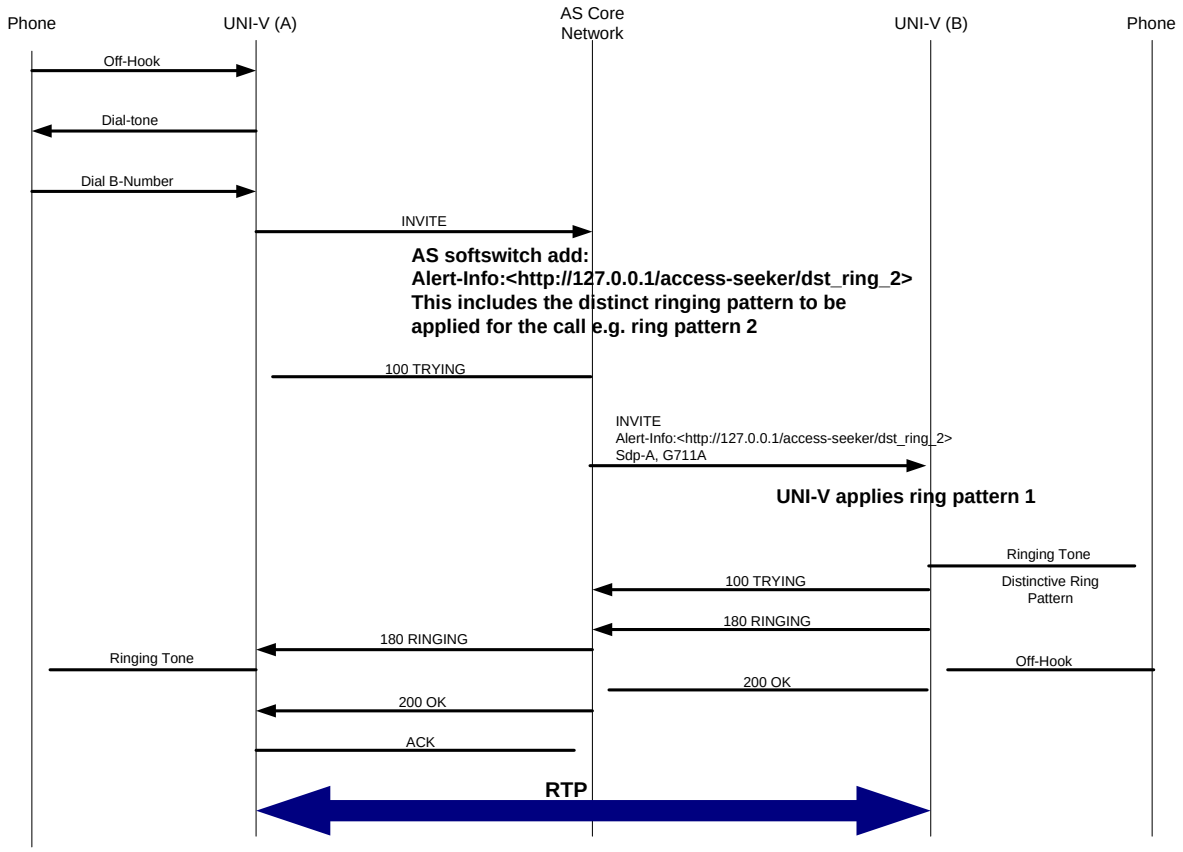


Figure 23 - Distinctive Ringing

9.11. Calling Number Display

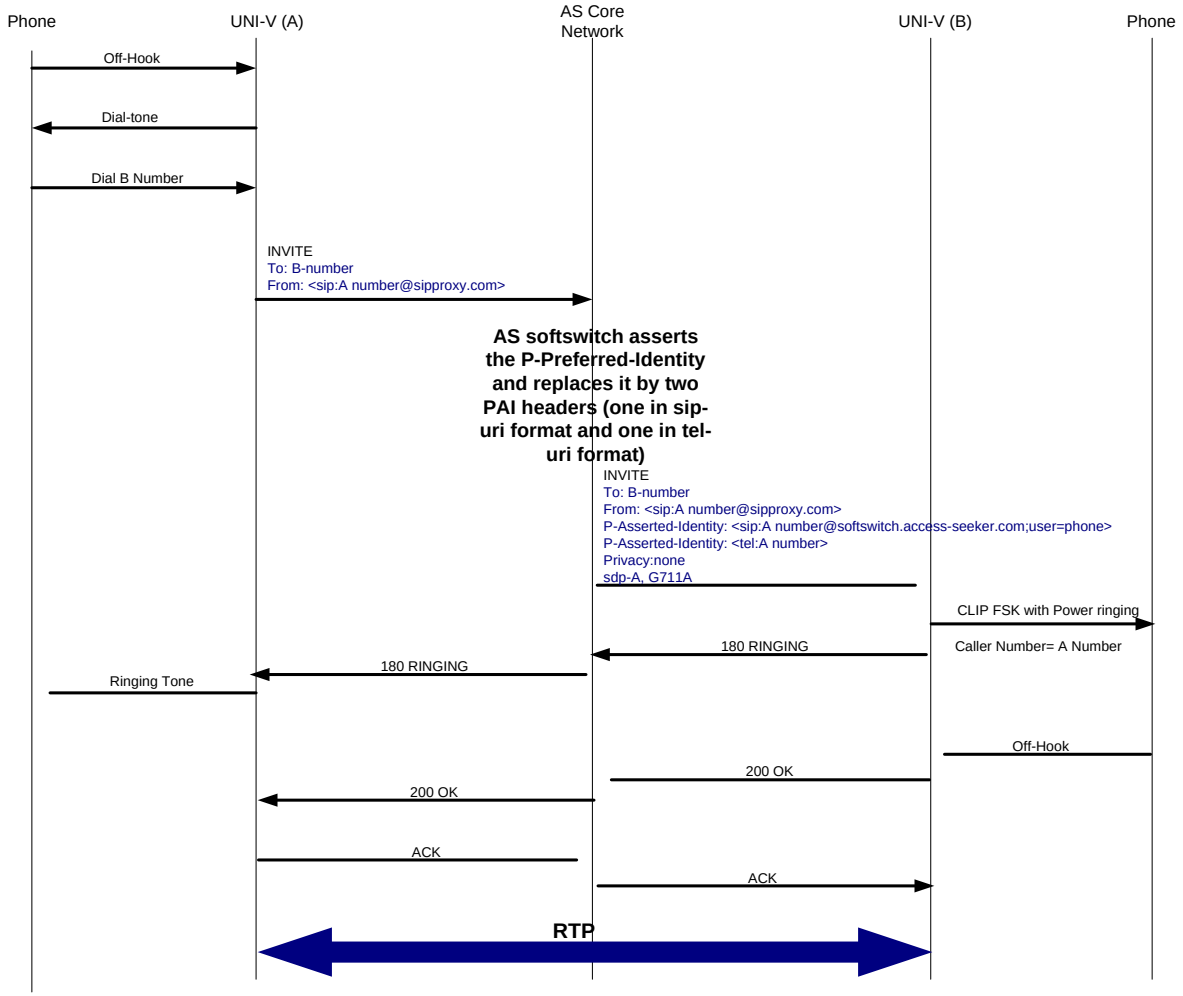


Figure 24 - CLIP SIP Flow

9.12. Calling Line ID Restriction (CLIR)

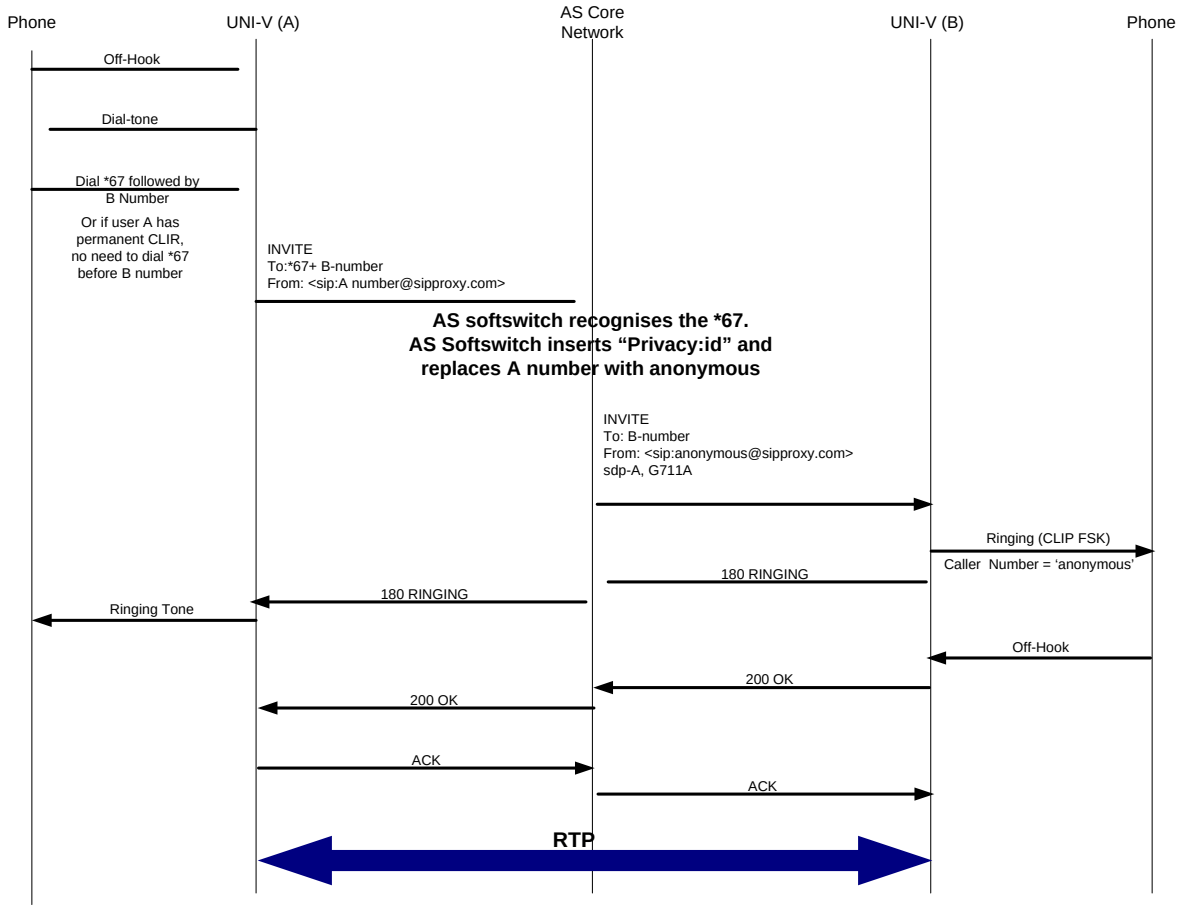


Figure 25 - CLIR SIP Flow

9.13. Emergency Calling

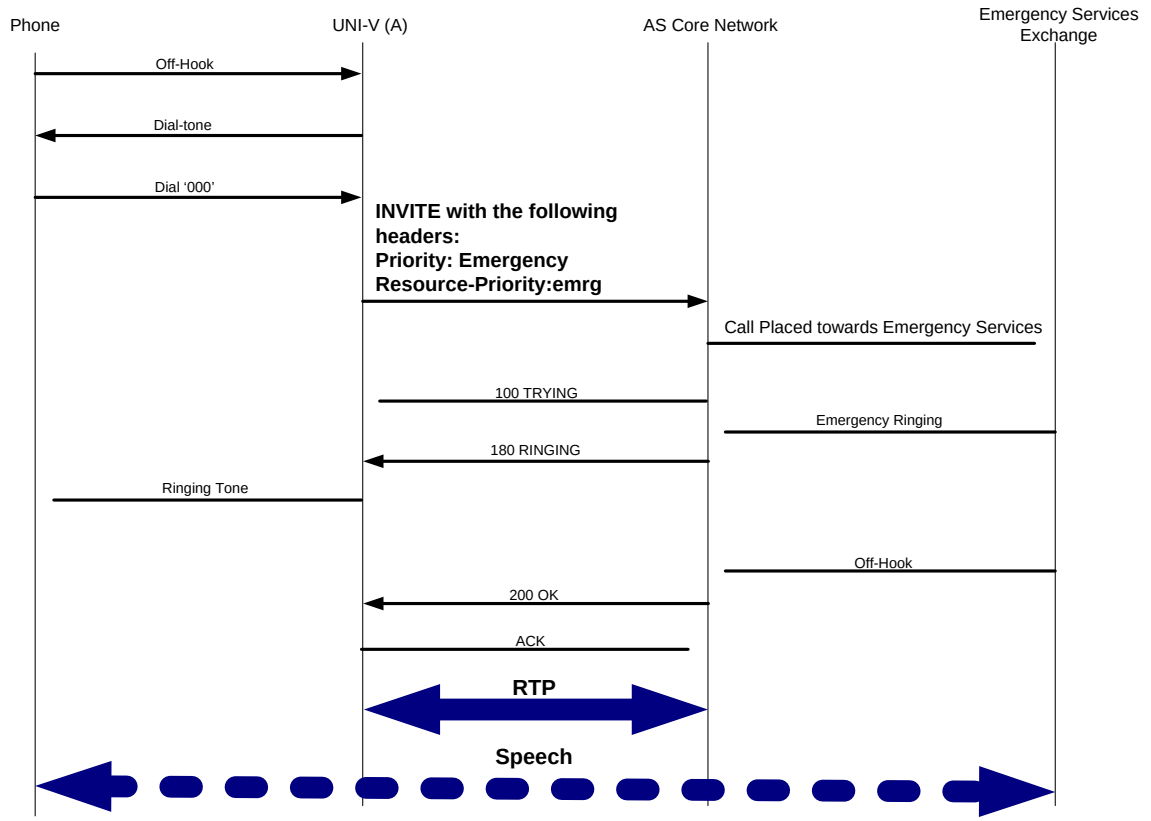


Figure 26 - Emergency Call SIP Flow

9.14. Message Waiting Indication

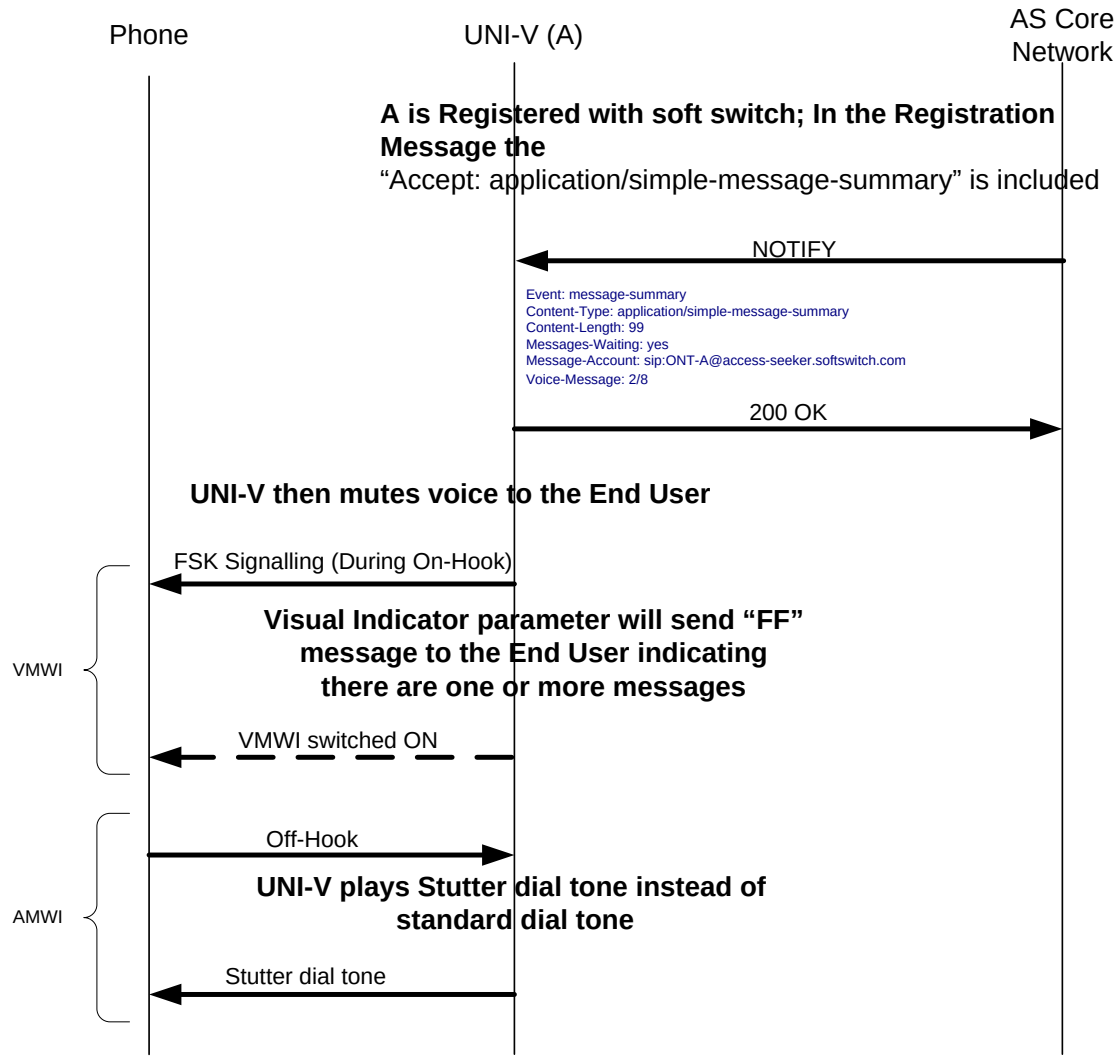


Figure 27 - Message Waiting Indication SIP flow

9.15. Abandoned Call

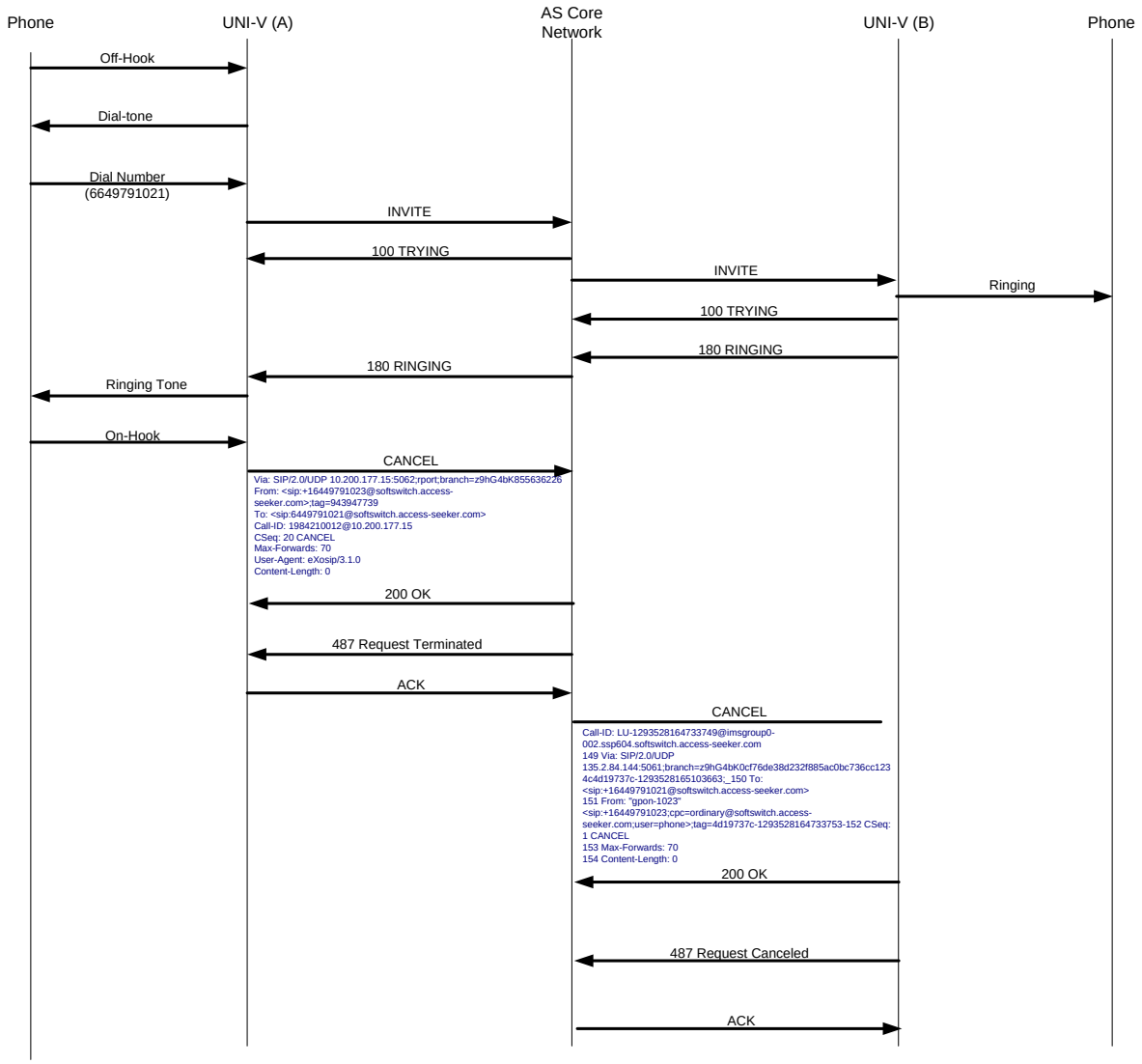
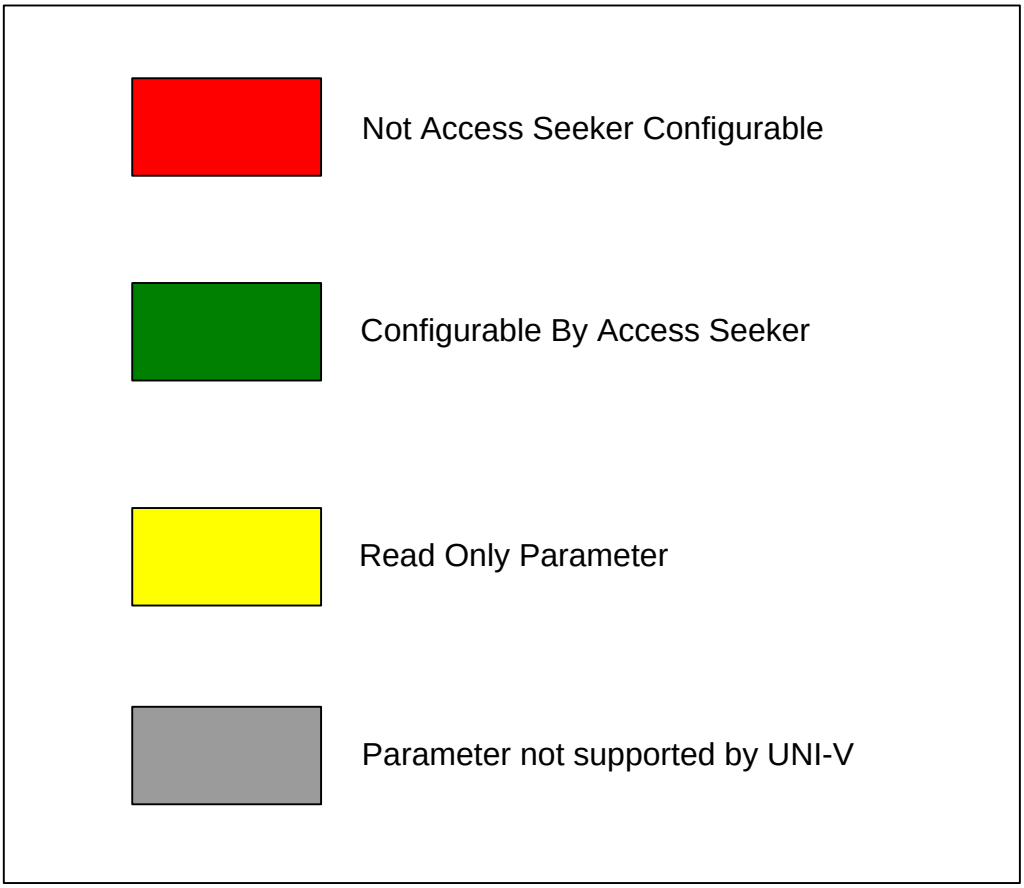


Figure 28 - Abandoned Call Flow

10. TR-069 Parameters Configuration

This section lists all objects and their parameters that are currently supported by the UNI-V.
It describes each parameter, its default value and whether it may be writable or not as illustrated in the diagram below. Some parameters are displayed by the UNI-V as writable, however those parameters are not be supported by NBN Co and hence cannot be configured by access seeker.

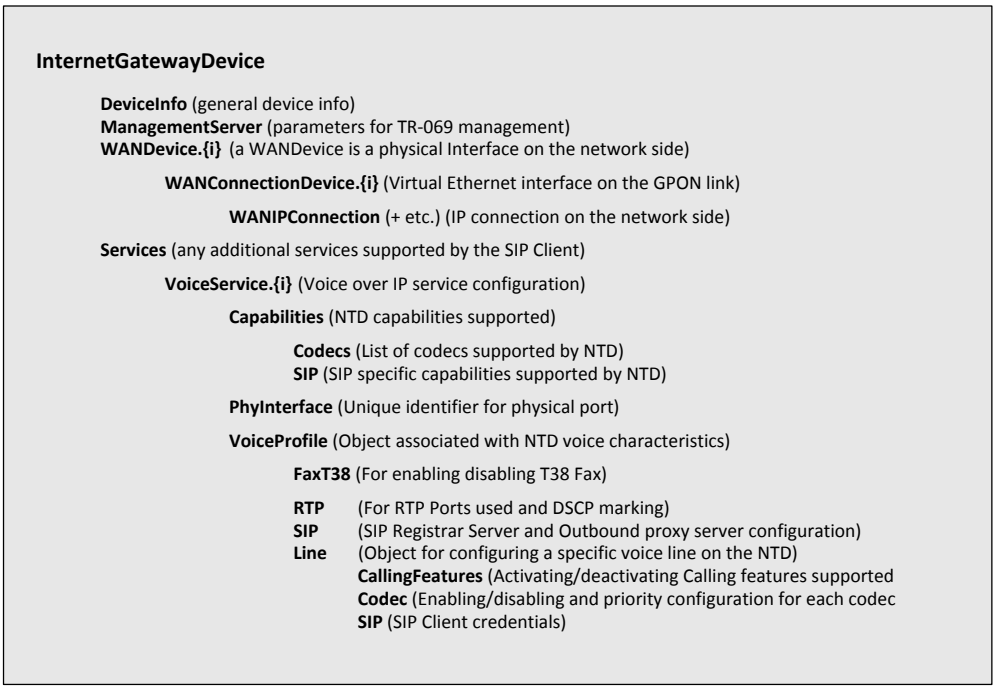
Access seeker should note that certain parameters in this section, such as ManufacturerOUI, are subject to change. Change to those parameters may affect access seeker's ACS ability to provision or manage end user services. It is recommended that access seeker assess and manage the impact of those parameters changing in an ongoing manner.



The configuration parameters described in this section are broken into two groups:

1) TR-098 configuration parameters
2) TR-104 configuration parameters

The TR-069 based object model that is supported by the UNI-V is shown below:



10.1. UNI-V TR-098 Configuration Parameters

InternetGatewayDevice

Parameter	Description	Write/Read	Default Value
LANDeviceNumberOfEntries	Number of LAN instances	Read	0
WANDeviceNumberOfEntries	Number of WAN instances	Read	1

InternetGatewayDevice.DeviceInfo

Parameter	Description	Write/Read	Default Value
AdditionalHardwareVersion	There is no additional hardware version supported	Read	NULL
AdditionalSoftwareVersion	There is no additional software version supported	Read	NULL
HardwareVersion[1]	Hardware version supported	Read	
SoftwareVersion[1]	Software version supported	Read	
Description[1]		Read	
Manufacturer[1]	NTD manufacturer	Read	ALCL
ManufacturerOUI[1]	NTD manufacturer identifier	Read	0019C7
ModelName[1]	The model name of the NTD	Read	GPON ONT
ProductClass[1]	NTD variant	Read	I-240G-R; Indoor NTD O-240G-P; Outdoor NTD

ProvisioningCode	Access seeker identifier and other provisioning information. On a new NTD install DHCP Option 43 will configure the UNI-V with its initial provisioning code to authenticate with the ACS. **Max is 63 characters.**	Read/Write	NULL
SerialNumber[1]	Serial number of the UNI-V. Each UNI-V will be represented with a unique serial number	Read	String
SpecVersion[1]	This parameter is deprecated by TR-098	Read	1.0

Note 1: The values for these parameters are examples only and may change from time to time.

InternetGatewayDevice.ManagementServer

Parameter	Description	Write/Read	Default Value
ConnectionRequestURL	The HTTP URL the ACS uses to connect to the UNI-V. This is configured in the form: http://host:port/path. **Max is 255 characters.**	Read/Write	NULL
ConnectionRequestUsername	The Username the ACS uses to connect to an UNI-V using Connection Request. **Max is 63 characters.**	Read/Write	NULL
ConnectionRequestPassword	The password the ACS uses to authenticate with the UNI-V using Connection Request **Max is 63 characters.**	Read/Write Note Read will return an empty string.	NULL
Username	Username used by the UNI-V to authenticate with the ACS when initiating a connection. **Max is 63 characters.**	Read/Write	NULL
Password	The Password used by the UNI-V when connecting to the ACS. **Max is 63 characters.**	Read/Write Note Read will return an empty string.	NULL
PeriodicInformEnable	Enable or disable the UNI-V from periodically sending information to the ACS using the inform method. "1"= enabled "0"= disabled	Read/Write	1

PeriodicInformInterval	The duration in seconds before the UNI-V connects to the ACS. This will call the Inform method if the PeriodicInformEnable is enabled. **Unsigned Integer max value is 0Xffffffff (Hex).**	Read/Write	86400
URL	The URL used by the UNI-V to connect to the ACS. This is initially configured using DHCP Option 43 option code 1. **Max is 255 characters.**	Read/Write	Set by DHCP Option 43
ParameterKey	Specific for Motive ACS	Read	

InternetGatewayDevice.WANDevice.{i}.

Parameter	Description	Write/Read	Default Value
WANConnectionNumberOfEntries	Number of WAN instances	Read	1

InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.

Parameter	Description	Write/Read	Default Value
WANIPConnectionNumberOfEntries	Number of WAN IP instances	Read	1
WANPPPConnectionNumberOfEntries		Read	0

InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.

Parameter	Description	Write/Read	Default Value
AddressingType	The method used to assign the UNI-V's WAN IP address. Only "DHCP" option is supported.	Read/Write	DHCP
ConnectionStatus	The status of the network connectivity. Only the status "connected" is supported since ACS would not be able to read this value when not connected.	Read/Write	
ConnectionTrigger	Trigger used to establish IP connection.	Write/Read	AlwaysOn
ConnectionType	Specifies the connection type of the connection Instance.	Write/Read	Unconfigured
DNSEnabled	Enable/Disable DNS query.	Write/Read	1
DNSOverrideAllowed	Whether or not a manually set, non-empty DNS address can be overridden by a DNS entry received from the WAN. Default value is disabled.	Write/Read	0
DNSServer	DNS Server IP address. This parameter is set to the DNS IP address configured by DHCP. **Max is 64 characters.**	Write/Read	0.0.0.0
DefaultGateway	UNI-V default gateway. This parameter is set to the Default IP address configured by DHCP.	Write/Read	0.0.0.0
Enable	Enable/disable WAN instance.	Write/Read	1
ExternalIPAddress	External IP address used when Network Address Translation (NAT) is enabled. This parameter is set to the IP address configured by DHCP.	Write/Read	
LastConnectionError	This parameter indicates the reason for the last failed connection. Only "ERROR_NONE" is displayed.	Read	
MACAddress	The MAC address of the UNI-V. Each UNI-V has a unique MAC address.	Read/Write	

NATEnabled	Enable/Disable Network Address Translation. "1"= enabled "0"= disabled	Read/Write	0
Name	User-readable name of the connection.	Read/Write	
PortMappingNumberOfentries	The total number of port mapping entries	Read	0
PossibleConnectionTypes	The type of connections supported by the UNI-V for this connection instance. This parameter supports only "Unconfigured".	Read	Unconfigured
RSIPAvailable	This indicates if Realm IP is available for the UNI-V. This parameter is set to be disabled.	Read/Write	0
RouteProtocolRx	Routing protocol supported by the UNI-V. The NTD only supports the "OFF" value setting.	Read/Write	Off
SubnetMask	The UNI-V network subnet. This parameter is set to the subnet mask configured by DHCP.	Read/Write	

10.2. UNI-V TR-104 Configuration Parameters

InternetGatewayDevice.Services .VoiceService.{i}.

Parameter	Description	Write/Read	Default Value
VoiceProfileNumberOfEntries	Number of VoiceProfile instances.	Read	1

InternetGatewayDevice.Services .VoiceService.{i}.Capabilites

The overall capabilities that are supported by the UNI-V are summarised in the table below. All parameters are "READ", hence are not configurable.

Parameter	Description	Write/Read	Default Value
ButtonMap	UNI-V does not support button map. Default value of "0" indicates that this field is unsupported.	Read	0
DSCPCoupled	UNI-V marks the RTCP traffic differently from the RTP traffic. Default value of "0" indicates that this field is unsupported.	Read	0
DigitMap	UNI-V supports digit map. Default value of "1" indicates that this field is supported. Max 1024 characters enclosed within ()	Read	1
EthernetTaggingCoupled	RTCP traffic uses the same S-VLAN ID as the RTP traffic. Default value of "1" indicates that this field is supported.	Read	1
FaxPassThrough	FaxPassTHrough is enabled. The UNI-V does not support the parameter VoiceService.-{i}.VoiceProfile.{i}.FaxPassThrough.	Read	1
FaxT38	The UNI-V supports the parameter VoiceService.{i}.VoiceProfile.{i}.FaxT38. Default value of "1" indicates that this field is supported.	Read	1
MaxLineCount	Maximum total number of lines supported across all profiles supported by the UNI-V	Read	1
MaxProfileCount	Maximum number of distinct Voice Profiles supported by the UNI-V	Read	1
MaxSessionCount	Maximum number of voice sessions supported across all voice profiles and lines.	Read	2
MaxSessionsPerLine	Maximum number of voice sessions supported for any given line across all profiles.	Read	2
ModemPassThrough	ModemPassThrough is permanently enabled on the UNI-V. The VoiceService.-{i}.VoiceProfile.{i}.ModemPassThrough parameter is not supported and the parameter is not configurable.	Read	1
NumberingPlan	The UNI-V does not support VoiceService.{i}.-VoiceProfile.{i}.NumberingPlan object.	Read	0
PSTNSoftswitchOver	The UNI-V does not support the PSO_Activate Facility Action for calls to be switched to PSTN line.	Read	0
RTCP	RTCP is permanently enabled on the UNI-V. The VoiceService.{i}.VoiceProfile.{i}.RTP.RTCP object parameter is not supported or configurable.	Read	0
RTPRedundancy	The UNI-V does not support VoiceService.{i}.VoiceProfile.{i}.RTP.Redundancy object.	Read	0
Regions	The geographic region associated with this profile is "AU" representing Australia region.	Read	AU

RingGeneration	The UNI-V does not support VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Ringer object.	Read	0
SRTP	Secure RTP is not supported by the UNI-V, hence the UNI-V does not support VoiceService.{i}.VoiceProfile.{i}..RTP.SRTP.	Read	0
SignalingProtocols	Signalling protocol supported by the UNI-V is SIP.	Read	SIP
ToneGeneration	The UNI-V does not support VoiceService.{i}.-VoiceProfile.{i}.Tone.	Read	0
VoicePortTests	The UNI-V does not support VoiceService.{i}.PhyInterface.{i}.Tests object.	Read	0

InternetGatewayDevice.Services .VoiceService .{i}.Capabilities.Codecs.{i}.

In the capabilities object, the codec list includes all supported codecs by the UNI-V. This includes the bit rate supported for each codec, packetisation periods supported for each codec and whether or not silence suppression is supported for each codec.

G.711ALaw (This is the standard PSTN codec recommended for use in Australia)

Parameter	Values Supported
Bitrate	64000 (bits/seconds)
Codec	G.711ALaw
EntryID	1
PacketizationPeriod	10,20,30 (ms)
SilenceSuppession	1 (Supported)

G.711MuLaw

Parameter	Values Supported
Bitrate	64000 (bits/seconds)
Codec	G.711MuLaw
EntryID	2
PacketizationPeriod	10,20,30 (ms)
SilenceSuppession	1 (Supported)

G.729

Parameter	Values Supported
Bitrate	8000 (bits/seconds)
Codec	G.729
EntryID	3
PacketizationPeriod	20,30 (ms)
SilenceSuppession	1 (Supported)

InternetGatewayDevice.Services .VoiceService.{i}.Capabilities.SIP

Parameter	Description	Write/Read	Default Value
EventSubscription	The UNI-V does not support VoiceService.{i}.-VoiceProfile.{i}.SIP.EventSubscribe and VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.EventSubscribe.{i} objects. Set to "0" Disabled	Read	0
Extensions	SIP method extension supported by UNI-V.	Read	REFER,UPDATE,INFO
ResponseMap	The UNI-V does not support VoiceService.{i}.-VoiceProfile.{i}.SIP.ResponseMap. Set to "0" Disabled	Read	0
Role	The role of the NTS is a "UserAgent"	Read	UserAgent
Transports	The UNI-V support UDP as a SIP transport protocol.	Read	UDP
URISchemes	The UNI-V does not support any URI schemes beyond the URI schemes required by the SIP specifications.	Read	NULL

InternetGatewayDevice.Services. VoiceService.{i}.PhyInterface.{i}.

Parameter	Description	Write/Read	Default Value
Description	A description of the physical port.	Read	0x0201 (UNI-V-1) Or 0x0202 (UNI-V-2)
InterfaceID	A unique identifier of the physical port.	Read	1
PhyPort	The UNI-V physical port number	Read	1

InternetGatewayDevice.Services .VoiceService.{i}.VoiceProfile.{i}.

Note: There are no VoiceProfile and Line objects existing by default. A single VoiceProfile instance VoiceProfile.1 needs to be created by access seeker's ACS. Once the VoiceProfile is created, a single Line object will be created automatically.

Parameter	Description	Write/Read	Default Value
DTMFMethod	Method used by UNI-V to pass DTMF digits. UNI-V only supports InBand and RFC2833 **(Note that InBand and RFC2833 is case sensitive)**	Read/Write	InBand
DigitMap	A collection of numbering plan patterns that determine when dialling is complete. **Max 1024 characters enclosed within ()**	Read/Write	(***xx|*xx*x.#|*xx*x.*xx#|*xx*x.*x#|*31*xxxxxxxx|*xx#|#xx#|*#xx#|#001|**x.T|x.T)
DigitMapEnable	Enable/disable digit map parameter above. "0"= Disable	Read	1

	"1"=Enable		
Enable[1]	Enable/Disable all lines in the VoiceProfile object. - Disabled - Enabled **(Note: Enabled/Disabled are case sensitive)**	Read/Write	Disabled
Reset[1]	This will reset and re-initialize the line to perform start-up actions e.g. SIP Registration. "0"= Disable "1"=Enable	Read/Write	0
Name		Read/Write	
SignallingProtocol		Read	SIP
MaxSessions	The maximum number of simultaneous call sessions for all lines in the VoiceProfile object.	Read	2
NumberOfLines	The number of lines supported in this VoiceProfile object.	Read	1
Region	The geographic region associated with this profile is "AU" representing Australia region.	Read	AU

Note 1: For a UNI-V registered via SIP, a change in value for these parameters will trigger a SIP de-registration.

InternetGatewayDevice.Services .VoiceService.{i}.VoiceProfile.{i}.FaxT38

Parameter	Description	Write/Read	Default Value
Enable	Enable/disable T.38 Fax on the UNI-V Default value is disabled "0"	Read/Write	0

InternetGatewayDevice.Services .VoiceService.{i}.VoiceProfile.{i}.RTP

Parameter	Description	Write/Read	Default Value
DSCPMark	The DSCP marking of the outgoing RTP traffic	Read/Write	0[1]
LocalPortMax	Highest port number from the port number range for incoming RTP traffic.	Read	50100
LocalPortMin	Lowest port number from the port number range for incoming RTP traffic.	Read	50000
TelephoneEventPayloadType	This is only used in an SDP offer by the UNI-V for DTMF events if RFC2833 transmission of DTMF information is enabled. **0 to 128.**	Read/Write	97

Note 1: Different DSCP values should be used for SIP and RTP to ensure optimal layer 2 NBN performance. For example, DSCP values of 46 (EF) for RTP and 40 (CS5) for SIP could be used, as per RFC 4594 and Communications Alliance G632:2012.

InternetGatewayDevice.Services .VoiceService.{i}.VoiceProfile.{i}.SIP

Parameter	Description	Write/Read	Default Value
DSCPMark[1]	The DSCP marking used for outgoing SIP and other non-RTP traffic, such as CWMP.	Read/Write	0[1]
OutboundProxy[2]	Server or proxy that all SIP messages and responses are sent. A numeric IP address (xxx.xxx.xxx.xxx) or A fully qualified domain name (fqdn). If this parameter is empty, all SIP signalling traffic will use the ProxyServer parameter (below). **Max is 256 characters**.	Read/Write	NULL
OutboundProxyPort	Destination port used when connecting to the OutboundProxy.	Read	5060

ProxyServer[2]	The address of the SIP Proxy server where all SIP requests are sent to unless the OutboundProxy (parameter above) is configured. A numeric IP address (xxx.xxx.xxx.xxx) or A fully qualified domain name (fqdn). **Must not be empty.** **Max is 256 characters**.	Read/Write	NULL
ProxyServerPort[2]	Destination port used when connecting to the ProxyServer. **0 to 65535.**	Read/Write	5060
ProxyServerTransport		Read	UDP
RegistrarServer[2]	If the OutboundProxy parameter is empty, all SIP traffic uses the RegistrarServer address. If this parameter is empty, the ProxyServer parameter will be used. The RegistrarServer parameter must be configured with a value identical to the value set in the ProxyServer. **Max is 256 characters**.	Read/Write	NULL
RegistrarServerPort[2]	Destination port used when connecting to the RegistrarServer. This parameter must be identical with ProxyServerPort. **0 to 65535.**	Read/Write	5060
RegistrarServerTransport		Read	UDP
RegisterExpires[2]	UNI-V proposed registration expiration time. Sets Expires value of REGISTER requests. **Unsigned Integer max value is 0xFFFFFFFFUnit is seconds**	Read/Write	3600

RegistrationPeriod[2]	RegistrationPeriod is the interval at which NTD should send re-REGISTER messages. It is configurable and should be less than or equal RegisterExpires. **Unsigned Integer max value is 0xFFFFFFFFUnit is seconds.**	Read/Write	3240
UserAgentDomain[2]	The UNI-V domain. **Max is 256 characters**.	Read/Write	NULL
UserAgentPort	SIP signalling port number used by UNI-V. **0 to 65535.**	Read	5060
UserAgentTransport	Transport protocol to be used for incoming call control signalling. Only supports UDP.	Read	UDP

Notes:
1. Different DSCP values should be used for SIP and RTP to ensure optimal layer 2 NBN performance. For example, DSCP values of 46 (EF) for RTP and 40 (CS5) for SIP could be used, as per RFC 4594 and Communications Alliance G632:2012..
2. For a UNI-V registered via SIP, a change in value for these parameters will trigger a SIP de-registration.

InternetGatewayDevice.Services .VoiceService.{i}.VoiceProfile.{i}.Line.{i}

Parameter	Description	Write/Read	Default Value
CallState	Indicates the call state of the UNI-V. The following are the call states supported: • Idle • Calling • Ringing • Connecting • InCall • Disconnecting	Read	NULL
Enable	Enable/disable the Line object. - Disabled - Enabled **(Note: Enabled/Disabled are case sensitive)**	Read/Write	Disabled
PhyReferenceList	The UNI-V this Line object is associated with. The UNI-V will set this parameter as: • 1 to indicate UNI-V1	Read[1]	1
Status	Indicates the status of the UNI-V line. The UNI-V supports: Initializing, Registering, Unregistering, Error, Disabled and Up.	Read	NULL

Note 1: This value is indicated as writable within the UNI-V TR-104 schema, however the assigned value will be preserved within the UNI-V. It can be read but not written by an access seeker's ACS.

InternetGatewayDevice.Services .VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures

Parameter	Description	Read/Write	Default Value
CallTransferEnable	Enable/Disable both Attended and Unattended Call transfer **This Parameter must be disabled by Access Seekers.**	Read/Write	1
CallWaitingEnable	Enable/Disable call waiting feature.	Read/Write	1
CallerIDEnable	Enable/Disable Calling number display	Read/Write	1
MWIEnable	Enable/Disable message waiting visual and audio indicator.	Read/Write	1
MaxSessions	Specifies that 2 sessions are allowed by the interface.	Read	2
X_ALCALTE-LUCENT-COM_DirectConnectURI	If set (not null) a UNI-V off-hook event triggers sending an immediate INVITE with this value as the To address. Value must be the same as SIP To header value if user had dialled the number. Typically: sip:hotline@fqdn or sip:hotline@ipaddress **Max 256 characters**	Read/Write	NULL

InternetGatewayDevice.Services . VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Codec.List.{i}.

The parameters in this section are populated from the VoiceService.{i}.Capabilities.Codecs table.

G.711ALaw (This is the codec recommended for PSTN interconnect in Australia)

Parameter	Read/Write	Default Values
Bitrate	Read	64000 (bits/seconds)
Codec	Read	G.711ALaw
Enable	Read/Write	1 (enabled)
EntryID	Read	1
PacketizationPeriod	Read/Write	20 (ms)
Priority	Read/Write	1
SilenceSuppression	Read/Write	1 (enabled) **This parameter must be disabled by access seeker**

G.711MuLaw

Parameter	Read/Write	Default Values
Bitrate	Read	64000 (bits/seconds)
Codec	Read	G.711MuLaw
Enable	Read/Write	1 (enabled) **This parameter must be disabled by access seeker**
EntryID	Read	2
PacketizationPeriod	Read/Write	20 (ms)
Priority	Read/Write	2
SilenceSuppression	Read/Write	1 (enabled)

G.729

Parameter	Read/Write	Default Values
Bitrate	Read	8000 (bits/seconds)
Codec	Read	G.729
Enable	Read/Write	1 (enabled) **This parameter must be disabled by access seeker**
EntryID	Read	3
PacketizationPeriod	Read/Write	20 (ms)
Priority	Read/Write	3
SilenceSuppression	Read/Write	1 (enabled)

InternetGatewayDevice.Services . VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP

Parameter	Description	Read/Write	Default Value
AuthPassword[1]	SIP Authentication password. **Max is 48 characters**.	Read/Write	NULL
AuthUserName[1]	SIP authentication user name. **Max is 48 characters**.	Read/Write	NULL
URI[1]	SIP address of record (AOR). Typically: sip:username@fqdn or sip:username@ipaddress If the URI is configured with username but without "@ipaddress or "@fqdn", the UNI-V will automatically add an @ and will use the domain configured in VoiceService.{i}.VoiceProfile.{i}.SIP.UserAgentDomain. **Max is 256 characters.**	Read/Write	NULL

Note 1. For a UNI-V registered via SIP, a change in value for these parameters will trigger a SIP de-registration.

11. Definitions

The following words, acronyms and abbreviations are referred to in this document.

Term	Definition
AAA	Authentication, Authorization, Accounting
ACS	Auto-Configuration Server
ALU	Alcatel-Lucent
AMWI	Audible Message Waiting
AOR	Address of Record
API	Application Program/Programming Interface
AR	Automatic Recall
AS	access seeker
ASCII	American Standard Code for Information Interchange
ATA	Analogue Telephony Adaptor
AVC	Access Virtual Circuit
BBPSU	Battery Backup Power Supply Unit
BH	Busy Hour
CAC	Call Admission Control
CAS	CPE Alerting Signal
CE	Customer Equipment
CIR	Committed Information Rate
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Indication Restriction
CND	Calling Number Display
Connectivity Serving Area	A geographical region that is addressable using a single CVC
CPE	Customer Premises Equipment
CVC	Connectivity Virtual Circuit
CWT	Call Waiting
CWMP	CPE WAN Management Protocol
DHCP	Dynamic Host Configuration Protocol
DN	Directory Number
DNS	Domain Name Service
DTMF	Dial Tone Multi Frequency
FQDN	Fully Qualified Domain Name
FSK	Frequency Shift Keying
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
MTU	Maximum Transmission Unit
MWI	Message Waiting Indicator
NFAS	NBN Co Fibre Access Service
NNI	Network to Network Interface
NTD	Network Termination Device
NTP	Network Time Protocol
OSI	Open System Interconnection
OSS	Operating Support System
PCMA	Pulse Code Modulation using G.711 A-law codec
POI	Point of Interconnect
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
REN	Ringer Equivalence Number
RTP	Real-time Transport Protocol
R-Value	The value for quantitatively expressing speech quality

Term	Definition
SDP	Session Description Protocol
SIP	Session Initiated Protocol
S-TAG	Service Tag
TC	Traffic Class (Quality of Service Traffic Class)
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking
UA	User Agent
UDP	User Datagram Protocol
UE	User Equipment
UNI-V	User Network Interface - Voice
URI	Universal Resource Identifier
URL	Uniform Resource Locator
V-Series	ITU-T Recommendation (Data communication over the telephone network)
VBD	Voice Band Data
VID	Virtual Local Area Network Identifier
VLAN	Virtual Local Area Network
VMWI	Visual Message Waiting
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
Wholesale Broadband Agreement	An agreement entered into between NBN Co and access seeker for the purpose of access seeker acquiring services by NBN Co, including the NFAS.
XML	Extended Markup Language

12. Known issues

A number of issues pertaining to the current release of the UNI-V functionality have been observed. NBN Co intends to rectify these known issues in future UNI-V releases.

Please note that suggested workarounds proposed by NBN Co should be assessed by access seeker to determine the workaround's suitability to its environment. It is up to access seeker to make its own decisions about the suitability of workarounds proposed by NBN Co.

1) Call rejection

Overview
The UNI-V rejects incoming calls under specific conditions.

Issue
In the INVITE SDP offer, when the access seeker network offers 10 or more codecs for negotiation with the UNI-V and G.711A is not offered for negotiation within the first 10 codecs, the UNI-V rejects the offer and hence the call is rejected. The UNI-V only supports the G.711A codec.

Potential solution / work-around
Access seeker could operate its network in a manner that will either present the G.711A within the first 10 supported codecs, or restrict the number of codecs allowed to be negotiated with the UNI-V.

Assessment
NBN Co intends to expand the number of codecs allowed in the SDP in a future release of the UNI-V.

2) Register "302 Moved Temporarily" response not supported - UNI-V registration response 302 not being actioned)

Issue
On reception of a 302 Register response, the UNI-V does not resend REGISTER message to new destination.

Assessment
Redirect servers can be used to provide scalability and redirect message to the correct destination by sending a 302 response. For example Broadsoft uses network servers to redirect SIP messages to the correct application server by sending a 302 response.

Potential solution / work-around
UNI-V receipt of 302 responses can be avoided by:

a) Having a Session Border Controller (which performs the 302 redirect) between the UNI-V and the Redirect servers (typical deployment configuration)
b) Configuring the UNI-V to register with final destination rather than Redirect server.

3) Call Waiting suspend service code

Issue
The UNI-V has a hard coded Call Waiting suspend activation code *70 that may clash with an access seeker's softswitch feature activation code(s).

Potential solution / work-around
Avoid the use of, or reassign, softswitch *70 feature codes.

4) Session Retry Wait Interval

Overview
The UNI-V will retry failed sessions to attempt to redeliver events that it has previously failed to deliver and to allow the ACS to make additional requests in a timely fashion.

Issue
The UNI-V does not fully comply with the retry wait interval table specified in table 3, section 3.2.1.1 of the TR-069, Amendment 1 standard.

The UNI-V implements only the first 3 waiting retry intervals in a circular loop. This generates more traffic towards access seeker's network when the UNI-V does not receive a response to any requests.

Potential solution / work-around
There is no direct workaround at present. One way to reduce traffic is by setting the PeriodicInformInterval value on the UNI-V to a fairly long interval which will lower TR-069 periodic traffic across access seekers' network.

Assessment
NBN Co intends to fix this defect in future releases to fully comply with the retry waiting interval.

5) Option code 254 (DHCP Option 43) state from invalid to valid

Overview
UNI-V rejects authentication with ACS when DHCP OPTION 43 Option Code 254 is changed from invalid value to a valid value (using UNI-V default ALCL TR-069 serial number) during the DHCP lease renewal.

Issue
If access seeker happens to send an invalid sub Option 254 value, followed by a valid sub option 254 which exactly matches the default TR-069 serial number (the NTD's serial number), the UNI-V will reject authentication with access seeker's ACS.

Potential solution / work-around
This scenario is very unlikely as access seeker is unlikely to be using option code 254 at all if using the NTD hardware serial number for TR-069 identification.

Assessment
NBN Co intends to fix this issue in a future release of the UNI-V so that if option code 254 is used and the status changed from an invalid value to a valid value, the UNI-V will still be able to authenticate the ACS.

6) UNI-V RTCP "Interarrival Jitter"

Overview
The RTCP “Inter-arrival Jitter” reported by the UNI-V is inconsistent with measured jitter on the incoming RTP stream.

Issue
The RTCP inter-arrival Jitter has been analysed and compared with external measurements and a discrepancy between the values has been observed.

Potential solution / work-around
There is no workaround available at this point in time. An access seeker can implement their own VoIP performance verification by measuring traffic within their network.

Assessment
NBN Co intends to fix this issue in a future release of the UNI-V

7) TR-069 Manageability and DHCP Behaviour

Overview

An access seeker ACS architecture with specific network events that trigger a UNI-V DHCP discovery or lease renewal, may cause some or all of the following to occur:

1. UNI-V *Connection Request* username and password being reset to factory defaults,
2. TR-098 *Periodic Inform Interval* is reset – to 20 secs
3. ACS username and password are reset to the DHCP Provisioning Code (option 43, option code 2) as provided by the access seeker. This is consistent with current UNI-V behaviour.

Trigger events that can invoke this behaviour are an NTD reset (e.g. power off/on, software upgrade, remote reset) a network outage or changes in DHCP provided values for either the Provisioning Code or ACS URL served through subsequent DHCP lease cycles.

Issue
Potential impacts of these three behaviours are:

1. If the UNI-V Connection Request username and password do not match values used by the ACS, then asynchronous contact from the ACS to the UNI-V will not be possible (the ACS will have to wait for completion of the next Periodic Interval to make contact).

2. A Periodic Inform Interval of 20 secs may result in excess traffic towards the Access Seeker ACS.

3. If the UNI-V's ACS username and password are reset to the DHCP provided Provisioning Code then the ACS must accept the changed authentication credentials if it has authentication enabled. This is consistent with current UNI-V behaviour.

Note that the UNI-V parameters relevant to this issue are found in the TR-098 *InternetGatewayDevice.ManagementServer* and DeviceInfo objects.

Access seeker will not be affected in the following circumstances:

- ACS authentication (UNI-V to ACS) is not used and UNI-V Connection Request username and password (for ACS to UNI-V connection) remain as factory defaults.
- ACS authentication username is always the same as the DHCP provided Provisioning Code and these values do not change between DHCP lease cycles.
- DHCP OFFER/ACK does not contain Provisioning Code.
- The UNI-V Connection Request username and password are not default values but the ACS responds to relevant UNI-V events (e.g. 1 BOOT, 2 PERIODIC) by checking TR-098 *InternetGatewayDevice. ManagementServer* values and modifying these values if needed.

Access Seekers may be affected if:

- The UNI-V's value for ACS Username (set via the ACS) is different to the *ProvisioningCode* provided by DHCP and the UNI-V subsequently reboots (or a DHCP Discovery occurs).
- Values for DHCP provided Provisioning Code change between DHCP lease cycles.

Potential solution / work-around
The mitigation strategy for an affected access seeker is dependent on their ACS architecture e.g. authentication approach, use of Provisioning Code, single ACS or dual ACS.

The following options may provide a suitable workaround:

- Not using ProvisioningCode based authentication for initial UNI-V contact with customer's ACS (ACS username and password can subsequently be used).
- If DHCP provided Provisioning Code is used, ensure it is always consistent with ACS username.
- The customer ACS responds to relevant TR-069 events (e.g. 1 BOOT, 2 PERIODIC) by checking and resetting non-default values for UNI-V Connection Request username/password and Period Inform Interval.
- If authentication is not required but Provisioning Code is present, do not configure the ACS username to an alternate value.
- Set default values for UNI-V Connection Request username/password with those provided by NBN Co.

Further, service manageability for a UNI-V can be returned via an NBNCo UNI-V factory reset. A UNI-V service reconfiguration by the Access Seeker's ACS should then occur in response to the UNI-V "0 BOOTSTRAP" message.

Assessment
This issue is currently under investigation.