# TR-069 on Yealink IP Phones

This technote mainly provides a general introduction of TR-069 (Technical Report 069) and the way of enabling the TR-069 on the Yealink IP phones. It also provides the supported RPC methods and the information of TR-111. The information in this document is restricted to the following Yealink IP phone models with firmware version 71 or later:

- SIP-T2xP IP Phones

- SIP-T3xG IP Phones

- SIP-T4X IP Phones

- VP530 IP Video Phones

- W52P IP DECT Phones (with firmware version 30 or later)

The following takes the SIP-T28P IP phone as an example.

TR-069 Introduction

TR-069 is a technical specification, which is defined by the Broadband Forum. It defines a mechanism that encompasses secure auto-configuration of a CPE (Customer-Premises Equipment), and also incorporates other CPE management functions into a common framework. TR-069 uses common transport mechanisms (HTTP and HTTPS) for communication between CPE and ACS (Auto Configuration Servers). The HTTP(S) messages contain XML-RPC methods defined in the standard for configuration and management of the CPE. The protocol addresses different Internet access devices such as modems, routers, gateways, set-top boxes, and VoIP-phones for the end-users.
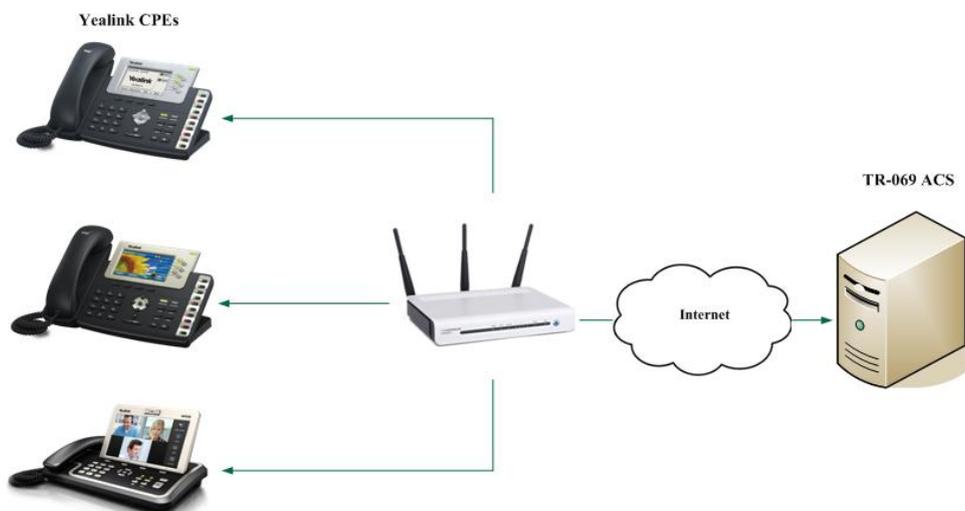
TR-069 Schematic Design

Why Use TR-069?

TR-069 is an application layer protocol, which has broad applicability and no access restriction. TR-69 standard allows the subscriber to manage all devices on a common platform regardless of its device type and manufacturer. Its specifications ensure that the device can be easily and securely configured, activated and managed from a console in the service provider's network. This allows the service provider to provide an efficient and cost effective deployment of services.

Configuring the TR-069 Feature on the IP Phone

TR-069 feature is disabled on the IP phone by default. You can enable or disable the TR-069 feature using the configuration files or web user interface.

To configure TR-069 using the configuration files:

1. Set the following parameters:

Parameter	Description	Valid Value	Default Value
managementserver.enable	Enables or disables the TR-069 feature on the phone.	Boolean	0
managementserver.username	Specifies the username used for HTTP authentication against the ACS.	String	Blank
managementserver.password	Specifies the password used for HTTP authentication against the ACS.	String	Blank
managementserver.url	Specifies the URL of ACS used to establish the TR-069 session with the ACS.	String	Blank
managementserver.connection_request_username	Sets the username used to authenticate the incoming connection requests.	String	Blank
managementserver.connection_request_passwor	Sets the password used to authenticate the incoming connection	String	Blank

| Parameter	Description	Valid Value	Default Value
d	requests.		
managementserver.periodic_inform_enable	Enables or disables the phone to report its configuration information to the ACS.	Boolean	1
managementserver.periodic_inform_interval	Sets the interval (in seconds) to report its configuration information to the ACS.	Integer	60

2. Store the configuration files to the root directory of the configuration server.

The following is an example of configuring VPN in the configuration file:

managementserver.enable = 1

managementserver.username = user123

managementserver.password = test123

managementserver.url = http://10.3.2.125:8080/acsm

managementserver.connection_request_username = phoneuser

managementserver.connection_request_password = connection

managementserver.periodic_inform_enable = 1

managementserver.periodic_inform_interval = 120

To configure TR-069 via web user interface:

1. Log in the web user interface with the administrator privilege.

2. Click on **Settings**->**TR069**.

3. Configure the parameters in the corresponding fields.

3
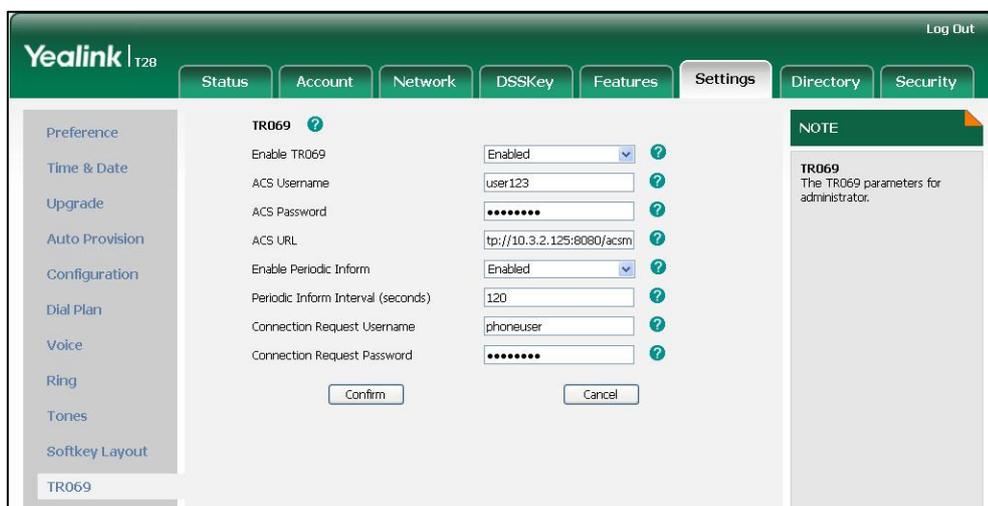
4. Click **Confirm** to accept the change.

After configurations, the phone establishes the TR-069 session with the ACS.

Supported TR-069 RPC Methods

The RPC (Remote Procedure Call) method defines a generic mechanism that is used for bi-directional communication between a CPE and an ACS. An ACS can get or set parameters to configure and monitor the CPE by using the RPC methods.

The following table provides a description of RPC methods supported by the Yealink IP phones:

RPC Method	Description
GetRPCMethods	This method is used to discover the set of methods supported by the CPE.
SetParameterValues	This method is used to modify the value of one or more CPE parameters.
GetParameterValues	This method is used to obtain the value of one or more CPE parameters.
GetParameterNames	This method is used to discover the parameters accessible on a particular CPE.
GetParameterAttributes	This method is used to read the attributes associated with one or more CPE parameters.
SetParameterAttributes	This method is used to modify attributes associated with one or more CPE parameters.
Reboot	This method causes the CPE to reboot.
Download	This method is used to cause the CPE to download a specified file from the designated location. File types supported by the Yealink IP phones are: ● Firmware Image ● Configuration File
Upload	This method is used to cause the CPE to upload a specified file to the designated location. File types supported by the Yealink IP phones are: ● Configuration File ● Log File
ScheduleInform	This method is used to request the CPE to schedule a one-time Inform method call (separate from its

RPC Method	Description
	periodic Inform method calls) sometime in the future.
FactoryReset	This method resets the CPE to its factory default state.
TransferComplete	This method informs the ACS of the completion (either successful or unsuccessful) of a file transfer initiated by an earlier Download or Upload method call.
AddObject	This method is used to add a new instance of an object defined on the CPE.
DeleteObject	This method is used to remove a particular instance of an object.

The ACS supports a variety of functionalities to manage a collection of phones using the above RPC methods, the following primary capabilities are included.

Auto-configuration and dynamic service provisioning

The ACS can provision a phone or collection of phones based on a variety of criteria. Different phone models can be configured using the uniform parameters. Phone can be provisioned at the initial connection and re-provision at any subsequent time. The ACS can also check the provision status (success or failure).

Firmware image management

Phone firmware can be upgraded or downgraded by downloading the firmware file from the ACS. TR-069 also provides mechanisms for version identification and file download initiation (ACS initiated downloads and optional phone initiated downloads). The ACS can be notified of the success or failure of a file downloading.

Status and performance monitoring

The ACS can use the GetParameterValues and GetParameterAttributes methods to monitor the phone's status and performance statistics. TR-069 also defines a set of mechanisms that allow the phone to actively notify the ACS of changes to its state.

Diagnostics

For troubleshooting purposes, the phone can send diagnostic information such as network status to the ACS, or the ACS can execute the defined diagnostic tests to get the information from the phone.

TR-111 Support

TR-111 standard defines two mechanisms that extend the CWMP defined in TR-069 to enhance the ability to remotely manage devices, which are connected via a LAN through an Internet gateway.

The two mechanisms are briefly summarized as follows:

- **Device-Gateway Association:** Allows an ACS managing a device to identify the associated gateway through which that device is connected.

- **Connection Request via NAT Gateway:** Allows an ACS to initiate a TR-069 Session with a device that is operating behind a NAT gateway.

Device-Gateway Association

The CPE cannot be contacted directly because they are not exposed to the internet. This mechanism is used to associate the CPE with the gateway which the CPE is connected. This association is communicated to the ACS in the Inform or Discover messages sent by the CPE, then the ACS can determine the identity of the gateway and establish sessions with the gateway. The connecting gateway must conform to the TR-111 specification.

Connection Request via NAT Gateway

When the CPE is located behind a NAT gateway and allocated a private address through the NAT gateway, the CPE must communicate its NAT binding to the ACS, then the ACS can initiate a session with the CPE. To accomplish the communication, the ACS must be associated with a STUN server that is used to require a new UDP-based Connection Request mechanism.

ACS Specific Information

Yealink IP phones can work properly with various ACS. For more information about the supported ACS, contact the Yealink technical support.

Data Model

Most of the configuration and diagnostics is performed through setting and retrieving the value of the phone parameters. These are organized in a well defined hierarchical structure that is more or less common to all phone models. For more information about the common and customized phone parameters, refer to the phone-specific document *Yealink_TR-069_DataModel.xls*. Contact the Yealink technical support for the data model file. Each of the parameters is marked as writable or non-writable. The phone does not permit the change of any parameter marked as read-only. Values applicable for the parameter, their type and meaning are also precisely defined in the document.

Normative References

TR-069: http://www.broadband-forum.org/technical/download/TR-069_Amendment-3.pdf

TR-104: http://www.broadband-forum.org/technical/download/TR-104.pdf

TR-106: http://www.broadband-forum.org/technical/download/TR-106_Amendment-3.pdf

TR-111: http://www.broadband-forum.org/technical/download/TR-111.pdf