TOBY-L2 series

Networking modes

Application note

Abstract

This document describes the two operational modes of the TOBY-L2 / MPCI-L2 module and how to provide connectivity to customer modems.

www.u-blox.com

UBX-14000479 - R05

Document information

Title	**TOBY-L2 series**	
Subtitle	Networking modes	
Document type	Application note	
Document number	UBX-14000479	
Revision and date	R05	10-Jun-2020
Disclosure restriction		

Product status	**Corresponding content status**	
Functional sample	Draft	For functional testing. Revised and supplementary data will be published later.
In development / Prototype	Objective specification	Target values. Revised and supplementary data will be published later.
Engineering sample	Advance information	Data based on early testing. Revised and supplementary data will be published later.
Initial production	Early production information	Data from product verification. Revised and supplementary data may be published later.
Mass production / End of life	Production information	Document contains the final product specification.

This document applies to the following products:

Product name
TOBY-L2 series
MPCI-L2 series

Contents

1 Introduction

TOBY-L2 / MPCI-L2 are Radio Access Technology (RAT) modules capable of operating in 2G, 3G and 4G mobile networks. Regardless of the currently selected RAT, the packet switched connectivity over the USB virtual Ethernet interface may be established in two different networking modes:

- **Bridge mode**: the IP termination of the data connectivity is on the customer's application processor and the module acts as a bridge device (similar to a USB dongle).
- **Router mode**: the IP termination is placed on the module itself. In this configuration the data connectivity of the customer's application processor is provided through routing procedures. The module is operating as a mobile router.

This document describes the two operating modes and how the IP connectivity is provided. In addition, the document provides additional information regarding:

- Development strategies for a reference connection manager useful in bridge mode.
- Description of the NAT (Network Address Translation) configuration useful in router mode.
- Description of the IPv6 configuration in bridge mode.
- Dial-up IPv4 configuration.
- How to increase the throughput on Linux OS.

For the sake of clarity, the u-blox cellular module is also referred to as the "target", while the device connected to it is called the "DTE" (Data Terminal Equipment). The physical connection between the target and the DTE is established through the USB interface, which supports different logical interfaces (RNDIS, CDC-ECM, SAP port and CDC-ACM).

The following symbols are used to highlight important information within the document:

☞ An index finger points out key information pertaining to module integration and performance.

⚠ A warning symbol indicates actions that could negatively impact or damage the module.

2 Bridge mode

2.1 General description

In bridge mode the target acts as a bridge device between the mobile network and the DTE: the IP termination of the data connection is placed on the DTE network subsystem. For each active PDP context or EPS bearer, the DTE assigns (i.e. “binds”) the IP address to its USB virtual Ethernet interface and configures its routing rules. Each IP address associated with an active PDP context/EPS bearer is granted to the target by the mobile network, and it shall be retrieved through appropriate AT commands. In bridge mode the PDP context/EPS bearer sets up a bridge between the cellular network and the USB interface: this is defined as bridge PDP context/EPS bearer.

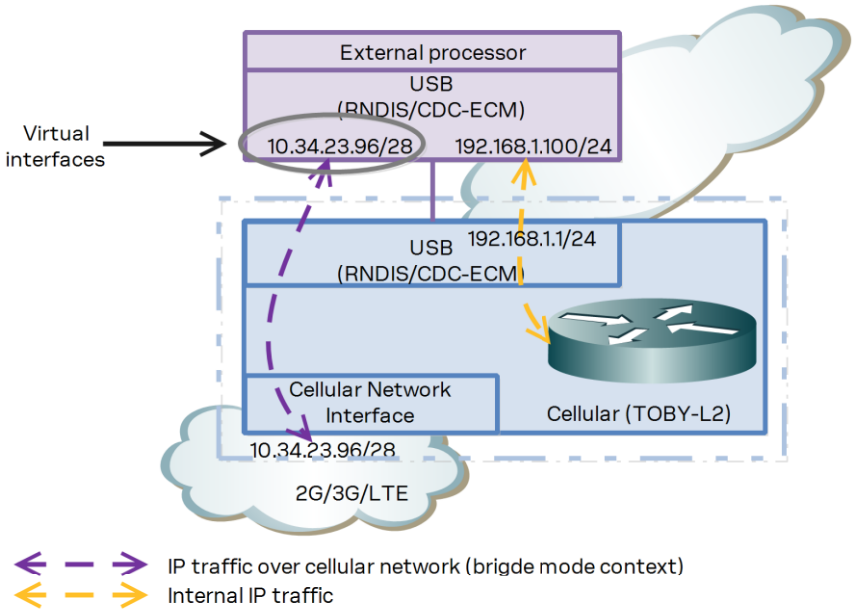


Figure 1: Bridge mode, single PDP context

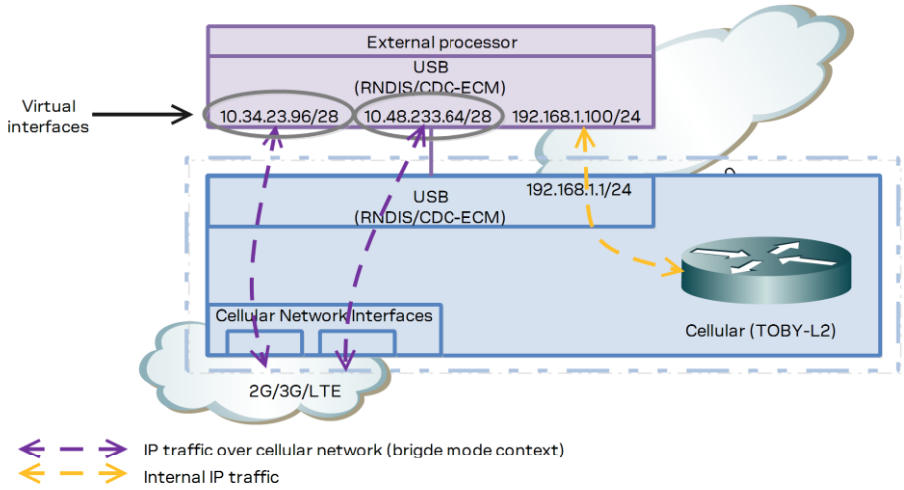


Figure 2: Bridge mode, multiple PDP contexts

Since several PDP context/EPS bearers can be activated, multiple IP addresses can be specified on the same physical interface by the use of interface aliases in Windows based systems and/or virtual interfaces in Linux based systems. The target is able to handle up to 8 different PDP contexts/EPS bearers.

2.2 DTE connectivity

This section explains how the DTE's network interfaces shall be configured to obtain connectivity through an active PDP context/EPS bearer. The steps for the configuration of Windows and Linux based systems are described. Finally, guidelines for the implementation of a Connection Manager application are provided.

The description covers both IPv4 and IPv6 addressing. Appendix A provides additional information on the configuration commands used in Windows and Linux systems.

2.2.1 IPv4

In bridge mode, the configuration of the DTE's network interfaces shall be performed manually because the automatic configuration through DHCP (Dynamic Host Configuration Protocol) server is not enabled by default. The automatic configuration through the DHCP server may be enabled for a preferred CID. For more details, see the section 2.3.

☞ See u-blox AT commands manual [1] for a detailed AT commands description and AT commands examples application note [2] for more examples on IPv4 configuration.

Perform the following steps for the configuration of every active PDP context/EPS bearer:

1. The DTE must retrieve the associated IP address with +CGPADDR or +CGDCONT, or +CGCONTRDP AT commands.
2. The DTE must assign the retrieved IP address to its USB virtual Ethernet interface as an alias.
3. The DTE must retrieve the network assigned DNS server addresses with +CGCONTRDP AT command.
4. In case of multiple active primary PDP contexts (each with its own IP address), each application running on the DTE should bind to a specific IP alias, to let the target forward the IP traffic to the desired PDP context.
5. The target creates a USB virtual Ethernet interface to reply to ARP (address resolution protocol) requests. The configured IP address has only local meaning. The DTE must retrieve this information with +UIPADDR AT command.
6. The DTE shall add a routing rule for its USB virtual Ethernet to ensure connectivity over the USB link. The gateway IP address of this rule must be the IP address retrieved at previous step. See Appendix A.1 and Appendix A.2 for additional information.

2.2.2 IPv6

☞ For a detailed description of link local and global address see appendix A.

The local connectivity is ensured by the automatic configuration of the link local address. The target's link local address is automatically set and can be retrieved with +UIPCONF AT command. The global connectivity is ensured by the global address, which should be univocal.

The global address consists of 128 bits, where the 64 bit long prefix is granted by the mobile network and the 64 bit long suffix is obtained from the less significant bits of the link local address.

In general terms, the global connectivity configuration of the network node shall be performed automatically by the IPv6 network through the use of DHCPv6 and/or IPv6 Neighbor Discovery Protocol (NDP), or manually by the user. Typically, the DHCPv6 is not supported on mobile networks; hence only two cases shall be analyzed. The IPv6 auto configuration with the NDP is performed within the handshake of Router Solicitation (RS) / Router Advertisement (RA) and Neighbor Solicitation (NS) / Neighbor Advertisement (NA) messages. All this messages are encapsulated into ICMPv6 packets.

The network node is broadcasting RS to locate routers on the connected link, while the routers are responding with the RA. The RA message provides the prefix of the announced network.

The network node is also broadcasting NS messages to determine the other nodes on the same physical link. These nodes shall be reached within link local addresses. The NS/NA handshake is equivalent to the IPv4 Address Resolution Protocol (ARP).

If the mobile network supports the IPv6 auto-configuration then the following steps must be followed for each successful PDP context activation:

- The Router Advertisement sent from the mobile network is forwarded to the USB virtual Ethernet interface of the DTE.
- The DTE processes the RA message and configures its global address and its routing rules. If the procedure is correctly completed then the host is provided with a global IPv6 address and with the IPv6 address (global or local) of the next-hop router. This global IPv6 address consists of the IPv6 prefix broadcasted by the RA, while the suffix is randomly generated. Furthermore, the host can be configured with a second IPv6 address, which can be retrieved by the use of the +CGDCONT AT command. This second IPv6 consists of the IPv6 prefix broadcasted by the RA, while the suffix is provided by the cellular network.
- Optionally the RA message can provide DNS server addresses. If present then the DTE shall apply the DNS configuration, otherwise the DTE should perform manual configuration.

If the mobile network does not support NDP then the DTE must perform a manual configuration for the global IPv6 address, next-hop address and DNS address for each successful PDP context activation:

- The prefix of the global address should be equal to the first 64 bits of the IP address retrieved with +CGPADDR AT command. The suffix should be equal to the last 64 bits of the USB virtual Ethernet interface link local address.
- The IPv6 address of the DNS server should be set. The user can choose between the set of the world-wide known DNS servers and addresses provided by the command +CGCONTRDP.
- The default route should be created toward a fake IPV6 address on the same network in order to forward the internet traffic on the USB link.
- To prevent continuous transmission of Neighbor Solicitation messages to this fake address the DTE should add it to its IPv6 neighbor list.

2.3 DHCP server configuration in bridge mode

In bridge mode the network auto-configuration through the DHCP server can be enabled only for a preferred EPS bearer / PDP context. The configuration is performed within two additional parameters of the +UBMCONF AT command. The first parameter is used to enable or disable the DHCP server; by default the DHCP server in bridge mode is disabled. The second parameter is used to configure the EPS/PDP context where to enable the DHCP server; when enabled the DHCP server is configured by default on CID=4, which in most of the cases represents the initial default EPS bearer.

Once the preferred EPS bearer / PDP context is activated, the DTE needs to issue a DHCP request to obtain the proper IP configuration. After the EPS bearer / PDP context deactivation the IP configuration associated to it is no more valid, hence the IP connectivity cannot be ensured.

The preferred EPS bearer / PDP context can be changed without the power cycle of the DCE. The new preferred CID will be used at the new EPS bearer / PDP context activation.

Only one preferred EPS bearer / PDP context can be specified at the time, hence the IP configuration of multiple EPS bearers / PDP contexts (expect the preferred) should be manually performed.

2.4 Connection manager development guidelines

The main tasks of the connection manager application running on the DTE are:

- Monitor the status of the PDP contexts/EPS bearers.
- Set up the IP configuration of the virtual interface for the activated PDP contexts (IP, gateway, DNS, routing rules).
- Unset the IP configuration of the virtual interface for the deactivated PDP contexts (IP, gateway, DNS, routing rules).

Three different implementation strategies for a connection manager are defined: “basic”, “smart” and “hybrid”.

Appendix A provides some examples of commands for setting IP address, gateway and DNS on Windows and Linux OS.

In bridge mode:

- The +UIPADDR AT command retrieves the gateway IP of an active PDP context.
- The +CGDCONT AT command retrieves the PDP context IP.

☞ Some network operators on their data networks support a MTU (maximum transmission unit) smaller than the standard 1500 bytes. In such cases then the IP data flow will incur IP fragmentation, thus lowering the throughput performance. In a network requiring a lower MTU then the customer should change his operating system to apply the new value over the virtual USB Ethernet link. For further details, see the Appendix F.

2.4.1.1 Basic implementation

The connection manager (CM) configures the DTE by taking into account the status of each PDP context/EPS bearer, retrieved with +CGDCONT and +CGACT AT commands.

The CM must properly set the IP, gateway and DNS addresses for the RNDIS and CDC-ECM interface aliases/virtual interfaces. Once the PDP context/EPS bearers are activated and the configuration is set, the connection manager must periodically poll the target to eventually update the settings or to track changes of the PDP contexts’ state, caused e.g. by the deactivation of PDP contexts commanded by the network due to roaming or temporary network’s issues.

The following list of instructions can be used as reference for the implementation on IPv4 based networks:

- In 2G/3G: define a PDP context with +CGDCONT AT command and activate it with +CGACT AT command. In 4G: the default initial PDP context is automatically activated during attach and it can be defined with AT+UCGDFLT AT command.
- Periodically poll the PDP contexts’ state (e.g. 5 s) with +CGACT read command (polling shall be maintained as long as the CM application is running).
- When the PDP context is active, get the needed IP address with +CGPADDR, +CGCONTRDP and +UIPADDR AT commands.
- Set up the OS with IP alias/virtual interfaces, routing rules and DNS configuration.
- If the PDP context is deactivated (it can be inferred by the information text response to the +CGACT read command) then remove all the settings for the related interface alias/virtual interface.

In the case of IPv6 based context the following instructions can be performed:

- If the mobile network supports NDP then set the DNS server if the DNS server is not present in the RA.

- Once the network sends the RA:
  - Find out the prefix granted by the mobile network with the +CGPADDR AT command.
  - Set the global IPv6 of the DTE: upper 64 bits of the network prefix plus the lower 64 bits of link local address of the context, which can be retrieved via +CGDCONT (or +CGCONTRDP) AT command.
  - Set the DNS servers.
  - To prevent continuous NS transmissions, set a route to a fake neighbor on the DTE and insert its address into the IPv6 neighbor list.

2.4.1.2 Smart implementation

This solution is event-driven: the CM application relies on URC notifications issued by the target at the AT command interface to track the changes of the connectivity through the mobile network.

The following list of instructions can be used as reference:

- In 2G/3G: define a PDP context with +CGDCONT and activate it with +CGACT AT commands.
- In 4G: the default initial PDP context is automatically activated during attach. It can be defined with AT+UCGDFLT.
- Enable the URC of +CGREG, +CEREG, and +CGEREP AT commands.
- Activate a PDP context with +CGACT AT command.
- Based on the URC issued by the target, handle the IPv4 and/or IPv6 configurations on the DTE. The activation of a context should trigger the configuration of the related interface alias/virtual interface, while the deactivation of a context should remove the configuration of the related interface alias/virtual interface.

2.4.1.3 Hybrid implementation

This approach is a simultaneous combination of the previous two solutions:

- Apply the “smart” approach by enabling and handling the URC related to registration and connectivity events.
- Apply the “basic” approach as a safety net with an appropriate polling timer (e.g. 20 s).

In this configuration the burden of the continuous polling mechanism is mitigated by the handling of the URC notifications. The polling mechanism with a larger timer offers a backup solution in case URC notifications are lost.

3 Router mode

3.1 General description

In the router mode, the IP termination is on the target: the module acts as a mobile network router and it is able to share its data connectivity through a private network over the USB interface. In router mode the PDP contexts/EPS bearers are connected to the module IP subsystem: this is defined as router PDP contexts/EPS bearers.

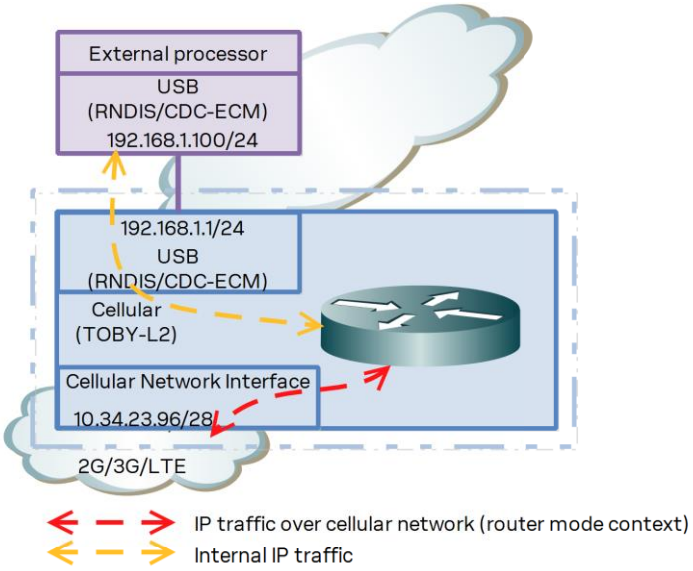


Figure 3: Router mode, single PDP context

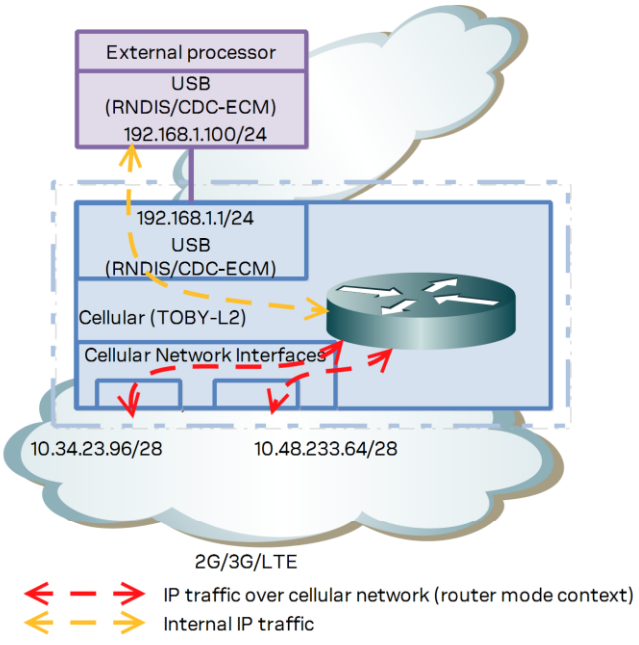


Figure 4: Router mode, multiple PDP contexts

☞ When the module is in bridge mode, several PDP contexts/EPS bearers can be configured as router contexts (see the u-blox AT commands manual [1] for PDP context/EPS bearer configuration).

3.2 DTE connectivity

This section provides information on how the DTE connectivity shall be configured in router mode. The description covers both IPv4 and IPv6 addressing. Appendix A provides additional information on the configuration commands used in Windows and Linux systems.

3.2.1 IPv4

In router mode the IP termination is placed on the target. For each PDP context/EPS bearer activation, the target creates an internal IP interface and assigns it the IP address of the activated PDP context/EPS bearer. The configuration of each internal IP interface can be retrieved with the +UIPADDR AT command.

Because the target is running a DHCP server on the USB link, the configuration of the DTE's virtual Ethernet interface can be performed automatically using a DHCP client or manually by specifying a static IP address.

The IP addresses of the virtual Ethernet interfaces of the target and of the DTE shall belong to the same private subnetwork to allow a two way communication.

The DTE is not aware of the target's mobile connectivity state and should retrieve it with at the +CGACT read command or any other equivalent AT command.

The DTE connectivity is achieved by forwarding the traffic between the target's USB virtual Ethernet interface and the internal IP interfaces. The IP traffic will be finally forwarded to an active PDP context/EPS bearer based on the target's routing table.

For each internal IP interface, the target will create a routing rule: the PDP contexts are activated consequentially and the activation history is stored in the target. The default gateway is always associated with the PDP context/EPS bearer that was activated first. Once this context/bearer is deactivated, the default gateway is re-associated with the next active PDP context/EPS bearer reported in the activation history.

The AT command +UIPROUTE shall be used to define static routes towards a specific PDP context/EPS bearer. The static routes may be set for a specific host IP or a specific network segment (subnetwork). The configuration of the static routes is volatile and it is lost at the target reboot.

The +UIPCONF, +UIPTABLES, +UIPROUTE and +UIPADDR AT commands configure the NAT, in this case port forwarding and IP masquerading), firewall, routing and of the USB virtual Ethernet interface.

Section 4.1 provides some reference examples.

3.2.2 IPv6

☞ Not supported by TOBY-L200 / TOBY-L210 / TOBY-L220 / TOBY-L280 product versions.

☞ See +UMNOCONF AT command in the u-blox AT commands manual [1] for more details.

In general terms, the global connectivity configuration of the network node shall be performed automatically by the IPv6 network through the use of IPv6 Neighbor Discovery Protocol (NDP). If the mobile network supports the IPv6 auto-configuration then the following steps must be followed for each successful PDP context activation:

- The Router Advertisement sent from the mobile network is processed. The information collected in the received RA are used to generate a RA, which is sent to the USB virtual Ethernet interface of the DTE. The Router Advertisement holds the prefix of the activated PDP context/EPS bearer.

- The DTE processes the RA message and configures its global address and its routing rules. If the procedure is correctly completed then the host is provided with a global IPv6 address and with the IPv6 address (global or local) of the next-hop router. This global IPv6 address consists of the IPv6 prefix broadcasted by the RA, while the suffix is randomly generated. Furthermore, the host can be configured with a second IPv6 address, which can be retrieved by the use of the +CGDCONT AT command. This second IPv6 consists of the IPv6 prefix broadcasted by the RA, while the suffix is provided by the cellular network.
- Optionally the RA message can provide DNS server addresses. If present then the DTE shall apply the DNS configuration, otherwise the DTE should perform manual configuration.

3.3 Conflicts between RNDIS/CDC-ECM private network and cellular network in router mode

Since several mobile providers use private network addressing, the cellular network may be in conflict with the private network associated with the USB virtual Ethernet interface (RNDIS/CDC-ECM). This may lead to an incorrect routing configuration.

To avoid loss of connectivity, the module should be properly configured:

Command	Response	Description
`AT+UIPCONF?`	`+UIPCONF: "10.18.130.1","255.255.255.0","10.18.130.100","10.18.130.254","FE80::2C60:20FF:FE56:2A2D/64"` `OK`	Retrieve the network configuration on the module USB virtual Ethernet interface.

`AT+UIPADDR=`	`+UIPADDR: 1,"ccinet0","5.168.120.242","255.255.255.255","",""`
	`+UIPADDR: 2,"ccinet1","46.12.30.162","255.255.255.255","",""`
	`+UIPADDR: 4,"ccinet3","10.18.130.248","255.255.255.255","",""`
	`OK`
		Retrieve the network configuration on the PDP context/EPS bearer.

`AT+UIPCONF="192.168.254.1","255.255.255.0","192.168.254.100","192.168.254.100"`	`OK`	If conflicts are present, the IP network configuration of the USB virtual Ethernet interface shall be adjusted to provide a new IP address/mask and a new range for the DHCP server running on the USB virtual Ethernet interface.
`AT+CFUN=1,1`	`OK`	Finally, the module should be rebooted to make effective the applied changes. It is worth noticing that also the host IP network configuration shall be verified and when needed adjusted (especially in the case of static addressing).

3.4 How to set the port forwarding on the module in router mode

To ensure that the DTE is reachable from the outside public network, port forwarding features shall be properly configured. For a proper configuration through the +UIPTABLES AT command, the following information shall be retrieved:

- the IP address of the host <host_IP>
- the port number on which the host is offering the service to the external network <host_port>
- the port number on which the target is listening <target_port>
- the protocol type used by the connection (e.g. 6 – TCP protocol, 17 – UDP protocol) <prot_num>

In the following table some examples are provided:

Example ID	AT command	Explanation
1	`AT+UIPTABLES="-t nat -A PREROUTING -p <prot_num> --dport <target_port> -i ccinet+ -j DNAT --to <host_IP>:<host_port>"`	Set port forwarding rules on all the PDP contexts/EPS bearers.
2	`AT+UIPTABLES="-t nat -D PREROUTING -p <prot_num> --dport <target_port> -i ccinet+ -j DNAT --to <host_IP>:<host_port>"`	Unset port forwarding rules on all the PDP contexts/EPS bearers.
3	`AT+UIPTABLES="-t nat -A PREROUTING -p <prot_num> --dport < target_port> -i ccinet<CID-1> -j DNAT --to <host_IP>:<host_port>"`	Set port forwarding rule on the PDP context/EPS bearer number CID. `<CID-1>` means CID number minus 1.
4	`AT+UIPTABLES="-t nat -A PREROUTING -p prot_num> --dport < target_port> -i ccinet<CID-1> -j DNAT --to <host_IP>:<host_port>"`	Unset port forwarding rule on the PDP context/EPS bearer number CID. `<CID-1>` means CID number minus 1.

☞ To avoid unreliable behavior, the interface parameter shall be always specified in the port forwarding rules

☞ The following TCP/UDP/ICMP connection timeouts are not affected by the command:

Timeout	Description	Default value [s]
`generic_timeout`	Generic timeout value	600
`tcp_timeout_syn_sent`	Timeout value related to the connection state SYN-SENT (defined in RFC 793 [14])	120
`tcp_timeout_syn_recv`	Timeout value related to the connection state SYN-RECEIVED (defined in RFC 793 [14])	60
`tcp_timeout_established`	Timeout value related to the connection state ESTABLISHED (defined in RFC 793 [14])	432000
`tcp_timeout_fin_wait`	Timeout value related to the connection state FIN-WAIT-1 and FIN-WAIT-2 (defined in RFC 793 [14])	120
`tcp_timeout_close_wait`	Timeout value related to the connection state CLOSE-WAIT (defined in RFC 793 [14])	60
`tcp_timeout_last_ack`	Timeout value related to the connection state LAST-ACK (defined in RFC 793 [14])	30
`tcp_timeout_time_wait`	Timeout after which the connection goes to the closed state	120
`tcp_timeout_close`	Timeout value related to the connection state CLOSE (defined in RFC 793 [14])	10
`udp_timeout`	Timeout value for UDP packets	300
`udp_timeout_stream`	Timeout value for UDP packets, when UDP stream is detected	300
`icmp_timeout`	Timeout value for IPv4 ICMP packets	30
`icmpv6_timeout`	Timeout value for IPv6 ICMP packets	30
`frag6_timeout`	Timeout value after the last fragmented IPv6 packet	60

4 Additional information

This section focuses on useful features which are common for both networking modes. Examples are provided in the next subsections.

☞ For a complete description of the AT commands see the u-blox AT commands manual [1].

4.1 AT commands examples

This section will provide some examples on how to configure the network connectivity on the target through the AT commands. Some AT commands can be used in both networking modes (i.e. +UBMCONF, +UIPCONF, +UIPADDR), while other AT commands are specific of each networking mode (i.e. +UIPTABLES).

4.1.1 Operational mode switch +UBMCONF

The networking mode can be set through the +UBMCONF command. The +UBMCONF AT command can also be used to identify the IP networking mode in which the target is operating.

☞ The new setting will be effective after the module reboot.

Command	Response	Description
`AT+UBMCONF=1`	`OK`	Set the router networking mode. This is the default and factory-programmed value.
`AT+UBMCONF=2`	`OK`	Set the bridge networking mode.
`AT+UBMCONF?`	`+UBMCONF: 2` `OK`	Get the networking mode. In the example the target is operating in bridge mode.
`AT+UBMCONF=2,1`	`OK`	Set the bridge networking mode and enable the IP auto-configuration of the DTE. The preferred CID is by default set to 4. To change the preferred CID a power cycle is not required.
`AT+UBMCONF=2,1,3`	`OK`	Set the bridge networking mode and enable the IP auto-configuration of the DTE. The preferred CID is set to 3. To change the preferred CID a power cycle is not required.

4.1.2 Target IP configuration +UIPCONF

The USB virtual Ethernet interface of the target is provided with a private IPv4 address and a link local IPv6 address. The IP addressing on the target can be configured through the +UIPCONF AT command in both networking modes:

- In router mode, the +UIPCONF AT command can configure or retrieve the private IPv4 address, the link local IPv6 address of the RNDIS interface and the range of the addresses provided by the DHCP server.
- In bridge mode, the +UIPCONF AT command can configure or retrieve the private IPv4 address of the USB virtual Ethernet interface (mainly for debugging purposes).

Command	Response	Description
AT+UIPCONF="192.168.2.1", "255.255.255.0","192.168. 2.100","192.168.2.100"	OK	In **router mode**: set the target IP address to “192.168.2.1”, the mask of the private network to “255.255.255.0”, the first IP address of the DHCP range to “192.168.2.100”, and the last IP address of the DHCP range to “192.168.2.100”. At least one client on the USB virtual Ethernet interface is supported. In **bridge mode**: set the target IP address to “192.168.2.1” and the mask of the private network to “255.255.255.0”. Other parameters are ignored.
AT+UIPCONF?	+UIPCONF: "192.168.5.1","255.255.255. 252","192.168.5.2","192.168.5.2","FE8 0::2C60:20FF:FE56:2A2D/64" OK	In **router mode**: get the target IP address “192.168.5.1”, the mask of the private network “255.255.255.252”, the first IP address of the DHCP range “192.168.5.2”, and the last IP of the DHCP range “192.168.5.2”. Due to the selected netmask, the range is limited to only one guest. The link local IPv6 address “FE80::2C60:20FF:FE56:2A2D/64” is finally reported. In **bridge mode**: get the target IP address “192.168.5.1”, and the mask of the private network “255.255.255.252”. Router-mode specific parameters (e.g. DHCP range), if previously configured, are also displayed but should be discarded.

4.1.3 IP configuration of the PDP contexts/EPS bearer +UIPADDR

The +UIPADDR AT command provides IP addresses of the interfaces for the mobile network connectivity. However, it is not able to provide information on an interface operating in bridge mode which has been configured by the mobile network only with an IPv6 address and without the IPv4 address.

The context ID is the same contained in the information text response of the +CGACT and +CGDCONT read commands.

Command	Response	Description
AT+UIPADDR=	+UIPADDR: 1,"usb0:0","5.168.120.242", "255.255.255.255","","" +UIPADDR: 4,"usb0:3","76.18.130.262", "255.255.255.255","","" OK	In **bridge mode**: get the list of the active PDP contexts/EPS bearers and associated IPv4 addresses. Two contexts are active. The first context has ID 1 and is associated with the virtual interface usb0:0. Its IPv4 address is 5.168.120.242. The second context has ID 4 and is associated with the virtual interface usb0:3. Its IPv4 address is 76.18.130.262.
AT+UIPADDR=	+UIPADDR: 1,"ccinet0","10.98.126.158" ,"255.255.255.0","","" +UIPADDR: 2,"usb0:1","10.26.129.73"," 255.255.255.0","","" OK	In **bridge mode** (bridge and router mode mixed contexts): get the list of the active PDP mixed contexts/EPS bearers and associated IPv4 addresses. Two contexts are active. The first special context has ID 1 and is associated with the interface ccinet0, which can be set by AT command AT+UDPDP to give the connectivity to the internal IP stack in bridge mode. Its IPv4 address is 10.98.126.158. The second context has ID 2 and is associated with the virtual interface usb0:1. Its IPv4 address is 10.26.129.73.

Command	Response	Description
AT+UIPADDR=	+UIPADDR: 1,"ccinet0","5.168.120.242","255.255.255.255","","" +UIPADDR: 2,"ccinet1","46.12.30.162","255.255.255.255","","" +UIPADDR: 4,"ccinet3","76.18.130.262","255.255.255.255","2001::2:200:FF:FE00:0/64","FE80::200:FF:FE00:0/64" OK	In **router mode**: get the list of the active PDP contexts/EPS bearers and associated IPv4/IPv6 addresses. Three contexts are active. The first context has ID 1 and is associated with the interface ccinet0. Its IPv4 address is 5.168.120.242. The second context has ID 2 and it is associated with the interface ccinet1. Its IPv4 address is 46.12.30.162. The third context has ID 4 and it is associated with the interface ccinet3. Its IPv4 address is 76.18.130.262, IPv6 global address is 2001::2:200:FF:FE00:0/64, its IPv6 link local address is FE80::200:FF:FE00:0/64.
AT+UIPADDR=4	+UIPADDR: 4,"usb0:3","76.18.130.262","255.255.255.255","","" OK	In **bridge mode** (IPv4 context): get the configuration of the active PDP context/EPS bearer with ID 4. This context is associated with the virtual interface usb0:3 and its IPv4 address is 76.18.130.262.
AT+UIPADDR=3	+UIPADDR: 3,"usb0:2","5.168.120.100","255.255.255.255","","" OK	In **bridge mode** (IPv4v6 context): get the configuration of the active PDP context/EPS bearer with ID 3. This context is associated with the virtual interface usb0:2 and its IPv4 address is 5.168.120.100.
AT+UIPADDR=2	ERROR	☞ In bridge mode (IPv6 context): for IPv6 only context the AT+UIPADDR command returns an error (It returns an error also when the PDP context is not active).
AT+UIPADDR=2	+UIPADDR: 2,"ccinet1","46.12.30.162","255.255.255.255","","" OK	In **router mode** (IPv4 context): get the configuration of the active PDP IPv4 only context/EPS bearer with ID 2. This context is associated with the interface ccinet1 and its IPv4 address is 46.12.30.162.
AT+UIPADDR=3	+UIPADDR: 3,"ccinet2","5.10.100.2","255.255.255.0","2001::1:200:FF:FE00:0/64","FE80::200:FF:FE00:0/64" OK	In **router mode** (IPv4v6 context): get the configuration of the active PDP IPv4v6 context/EPS bearer with ID 3. This context is associated with the interface ccinet2, with its IPv4 address is 5.168.120.100, IPv6 global address is 2001::1:200:FF:FE00:0/64, IPv6 link local address is FE80::200:FF:FE00:0/64.
AT+UIPADDR=2	+UIPADDR: 2,"ccinet1","","","2001::2:200:FF:FE00:0/64","FE80::200:FF:FE00:0/64" OK	In **router mode** (IPv6 context): get the configuration of the active PDP IPv6 context/EPS bearer with ID 2. This context is associated with the interface ccinet1 and its IPv6 global address is 2001::1:200:FF:FE00:0/64, IPv6 link local address is FE80::200:FF:FE00:0/64.
AT+UIPADDR=3	ERROR	☞ In router mode the context with ID 3 is not active; in bridge mode either the context with ID 3 is not active or it is active but IPv4 address has not been assigned to it.

4.1.4 IP tables configuration (router mode) +UIPTABLES

The +UIPTABLES AT command can be used to modify the firewall and port forwarding configuration of the target. All the rules are immediately applied and are also stored in the NVM (Not Volatile Memory). In case they shall be edited, it is recommended to delete the previously saved configuration with AT+UIPTABLES=.

Command	Response	Description
AT+UIPTABLES="-L -t nat"	Chain PREROUTING (policy ACCEPT) target prot opt source destination Chain OUTPUT (policy ACCEPT) target prot opt source destination Chain POSTROUTING (policy ACCEPT) target prot opt source destination MASQUERADE 0 -- anywhere anywhere MASQUERADE 0 -- anywhere anywhere MASQUERADE 0 -- anywhere anywhere MASQUERADE 0 -- anywhere anywhere MASQUERADE 0 -- anywhere anywhere MASQUERADE 0 -- anywhere anywhere MASQUERADE 0 -- anywhere anywhere MASQUERADE 0 -- anywhere anywhere OK	Get the rules of the nat table. ☞ The default table is filtered, hence the command "-L" is equivalent to "-L –t filter".
AT+UIPTABLES="-A PREROUTING -t nat -i ccinet3 -p tcp --dport 80 -j DNAT --to 192.168.1.100:22" AT+UIPTABLES="-A INPUT -p tcp -m state --state NEW --dport 80 -i ccinet3 -j ACCEPT"	OK	Both rules are required to set the port forwarding. The TCP traffic arriving on the port 80 of the interface ccinet3 is forwarded to the port 22 of the IP 192.168.1.200.
AT+UIPTABLES="-A INPUT -p tcp --destination-port 80 -j DROP"	OK	Set the blocking rule on the TCP traffic arriving on the port 80.
AT+UIPTABLES="-D INPUT 6"	OK	Delete the 6-th rules of the chain INPUT.
AT+UIPTABLES=" -A OUTPUT -p icmp --icmp-type 8 -j DROP"	OK	Block ICMP echo-request.
AT+UIPTABLES	OK	Delete the stored configuration.

4.1.5 Static routes configuration (router mode) +UIPROUTE

The +UIPROUTE command can be used to create/modify the static routes of the target. All the rules are immediately applied and are not stored in the NVM. If they need to be edited, it is recommended to delete the previous configuration. The +UIPROUTE command may overwrite the default routing rule or may lead to the loss of connectivity.

Command	Response	Description
AT+UIPROUTE?	+UIPROUTE: Kernel IP routing table	Get the rules of the IPv4 and IPv6 routing table.

Command	Response	Description
	Destination Gateway Genmask Flags Metric Ref Use Iface 192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 usb0 0.0.0.0 109.114.44.158 0.0.0.0 UG 0 0 0 ccinet0 Kernel IPv6 routing table Destination Next Hop Flags Metric Ref Use Iface fe80::/64 :: U 256 0 0 usb0 fe80::/64 :: U 256 0 0 ccinet0 ::1/128 :: U 0 0 1 lo fe80::200:ff:fe00:0/128 :: U 0 0 1 lo fe80::74f0:e8ff:feb3:af51/128 :: U 0 0 1 lo ff00::/8 :: U 256 0 0 usb0 ff00::/8 :: U 256 0 0 ccinet0 OK	
AT+UIPROUTE=""	+UIPROUTE: Kernel IP routing table Destination Gateway Genmask Flags Metric Ref Use Iface 192.168.1.0 * 255.255.255.0 U 0 0 0 usb0 default 37.182.69.142 0.0.0.0 UG 0 0 0 ccinet0 OK	List of the IPv4 routing rules. The default route is set within the ccinet0 (CID 0).
AT+UIPROUTE="add -net 140.105.63.0 netmask 255.255.255.0 dev ccinet1"	+UIPROUTE: OK	Set the static route for the 140.105.63.0/24 subnetwork towards the interface ccinet1 (CID 2).
AT+UIPROUTE="del -net 140.105.63.0 netmask 255.255.255.0 dev ccinet1"	+UIPROUTE: OK	Delete the static route for the 140.105.63.0/24 subnetwork towards the interface ccinet1 (CID 2).
AT+UIPROUTE="add -host 151.9.34.82 dev ccinet2"	+UIPROUTE: OK	Set the static route for the host 151.9.34.82 towards the interface ccinet1 (CID 2).
AT+UIPROUTE="del -host 151.9.34.82 dev ccinet2"	+UIPROUTE: OK	Delete the static route for the host 151.9.34.82 towards the interface ccinet1 (CID 2).
AT+UIPROUTE="del default"	+UIPROUTE: OK	Delete the default route.
AT+UIPROUTE="add default dev ccinet1"	+UIPROUTE: OK	Set the default route towards the interface ccinet1 (CID 2).

4.1.6 USB interface profile configuration +UUSBCONF

u-blox cellular modules provide several USB interface profiles. Each USB profile consists of some USB device classes, which differ from profile to profile.

As mentioned above, each USB profile implies a set of USB function.

Command	Response	Description
AT+UUSBCONF=?	+UUSBCONF: (0 ("6 CDC-ACM"),(""),()),(2 ("NETWORK, 3 CDC-ACM"),("ECM"),()),(3 ("NETWORK, 1 CDC-ACM"),("RNDIS"),()) OK	Available USB profiles.
AT+UUSBCONF=0	OK	Fairly back-compatible profile; the configuration only consists of six CDC-ACM.
AT+UUSBCONF=2,"ECM"	OK	Low/Medium throughput profile, the configuration includes a Network USB function (CDC-ECM), and three CDC-ACM; the presence of several USB functions limits the reachable data transfer throughput.
AT+UUSBCONF=3,"RNDIS"	OK	High throughput profile (default configuration); the configuration includes a Network USB function (RNDIS), and only one CDC-ACM; the presence of only one CDC-ACM allows a higher data transfer throughput.
AT+UUSBCONF=12,"ECM"	OK	Low/Medium throughput profile, the configuration includes a Network USB function (CDC-ECM), two CDC ACM, and one SAP port; the presence of several USB functions limits the reachable data transfer throughput.
AT+UUSBCONF=13,"RNDIS"	OK	High throughput profile (default configuration); the configuration includes a Network USB function (RNDIS), none CDC-ACM, and only one SAP port; the presence of only one SAP port allows a higher data transfer throughput.

The fairly back-compatible profile is also referred as legacy profile.

The following figures show how the interface is recognized on Windows systems:

1. Legacy mode:

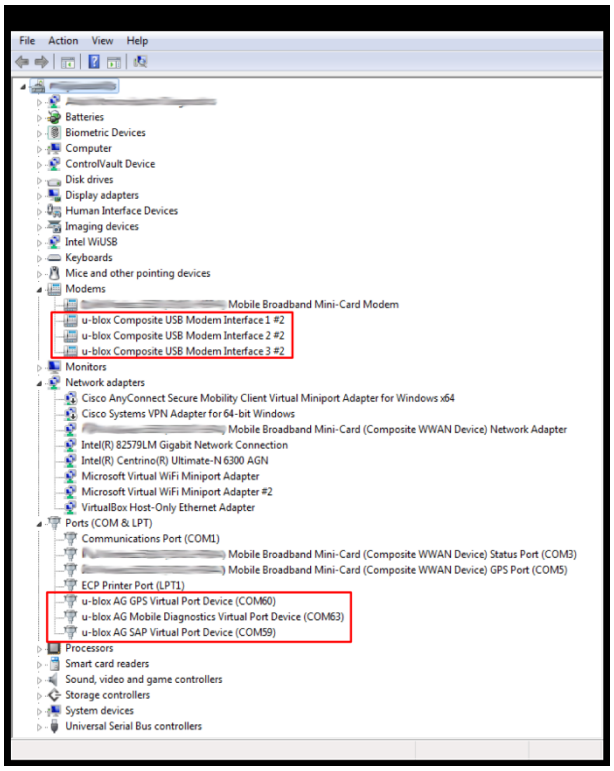


Figure 5: Legacy mode on Windows system

The Windows system recognizes 6 CDC-ACM interfaces: 3 of them are AT command interfaces. The additional 3 CDC-ACM interfaces are used for special purposes: GPS Virtual Port, Mobile Diagnostic Virtual Port and SIM Access Profile (SAP) Virtual Port.

2. CDC-ECM mode:

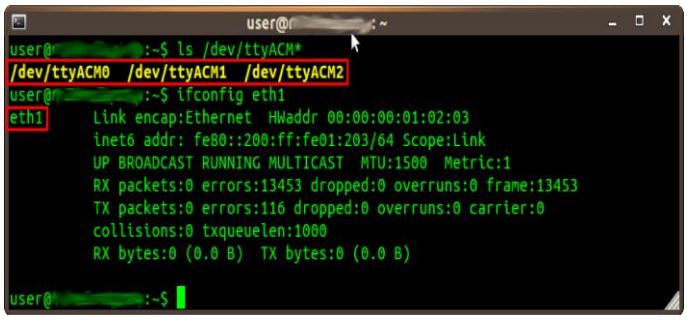


Figure 6: CDC-ECM mode on Linux system

The Linux system recognizes one CDC-ECM interface (eth1 interface in the list of network devices), and 3 CDC-ACM (3 AT command interfaces).

3. RNDIS mode:

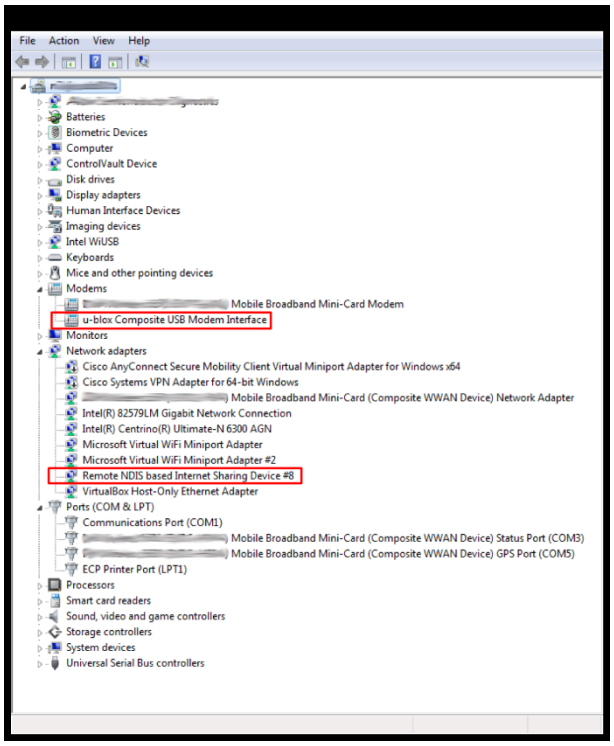


Figure 7: RNDIS mode on Windows system

The Windows system recognizes one RNDIS interface and one CDC-ACM interface (AT command interface).

The PPP connections may be established for every USB profile, since at least one CDC-ACM is available in every one.

4.1.6.1 USB interface connectivity for multiple modules

The high throughput profile considers one RNDIS interface. The MAC addresses at the target side and at the DTE side are randomly generated at every boot time. This configuration allows that several modules can be connected to the same DTE. At the physical level of the USB interface no conflict will be present.

The low/medium throughput profile considers one CDC-ECM interface. The MAC address at the target side is hardcoded, hence in this configuration only one target can be connected to a single DTE.

4.1.7 IPv6 firewall table configuration +UIP6TABLES

The +UIP6TABLES AT command can be used to modify the firewall and port forwarding configuration related to the IPv6 network of the target. All the rules are immediately applied and are also stored in the NVM. If they shall be edited, it is recommended to delete the previously saved configuration by means of the AT+UIP6TABLES= command.

Command	Response	Description
AT+UIP6TABLES?	Chain INPUT (policy ACCEPT) target prot opt source destination Chain FORWARD (policy ACCEPT) Target prot opt source destination Chain OUTPUT (policy ACCEPT) Target prot opt source destination OK	Get the rules of the filter table. ☞ The default table is filtered, hence the command "-L" is equivalent to "-L -t filter".
AT+UIP6TABLES="-A INPUT -p icmpv6 --icmpv6-type echo-request -j DROP"	OK	Drop the received echo requests.
AT+UIP6TABLES=	OK	Delete the stored configuration.

4.1.8 Advanced DNS configuration +UDNSCONF

The +UDNSCONF AT command can be used to configure additional settings of the Domain Name Server (DNS) resolver. This AT command enables:

- Setting a list of preferred DNS servers
- Setting a list of IP address that will be ignored as the resolution of required URL

The DNS servers in the preferred list will be used at first. The DNS requests are sent starting consequentially from the first entry to the last one, if available. Once the list of the preferred DNS servers is exhausted, the system DNS servers are used. The system DNS servers are obtained from the cellular network at PDP context/EPS bearer activation. The system DNS servers list will also contain the DNS servers of the Wi-Fi STA interface connected to the external hotspot.

Several mobile operator DNS servers can provide an IP address into "No such domain" replies. This IP address can correspond to an advertising/unwanted web page in response to a query for a not-found domain name, instead of the correct Non-Existent Domain (NXDOMAIN) response. The responses containing the IP addresses of the list to be ignored are considered by the DNS resolver as a NXDOMAIN response.

Command	Response	Description
AT+UDNSCONF=0	+UDNSCONF: "10.45.2.45" +UDNSCONF: "183.32.63.13" +UDNSCONF: "12.54.1.2" OK	Get the list of preferred DNS servers.
AT+UDNSCONF=11,"45.22.57.51"	OK	Append an IP address to the list of the ignored IP addresses.
AT+UDNSCONF=9	OK	Delete the list of preferred DNS servers.

☞ The list of the preferred DNS servers accepts IPv4 and IPv6 addresses.

☞ The list of the IP addresses to be ignored accepts IPv4 addresses.

☞ The preferred DNS server are applied to the internal contexts and internal clients (e.g. BIP, IMS)

For further information regarding the advanced DNS configuration, see Appendix D.

4.2 Dial-up connection

The module is able to perform dial-up connections supporting the Point-to-Point Protocol (PPP). The Point-to-Point Protocol provides a standard method for transporting multi-protocol datagrams over point-to-point links. The PPP connection is established between the target and the DTE in both router and bridge modes. In particular, the target performs as the PPP server, while the DTE performs as the PPP client.

The target supports both active and passive PPP negotiation modes. In active mode the server sends the first LCP Configuration Request message without waiting for the PPP client to do so, while in the passive mode the server waits for the PPP client to send the first LCP Configuration Request message before sending its own Configuration Request message. The target operates by default in passive mode. If the client does not send the first LCP packet within a given period (1 s), then the server (cellular module) will send the first LCP packet to the client. In particular, the value of the timeout is set to 1 s. If no LCP Configuration Response is received the request is repeated for at most ten times. The LCP Configuration Request is sent every 1 s.

It is worth noticing, that the number of dial-up connections depends on the active USB profile on the target. In the “High Throughput Profile” (AT+UUSBCONF=3,"RNDIS") there is only one CDC-ACM interface, hence only one dial-up connection can be established. In the “Low/Medium Throughput Profile” (AT+UUSBCONF=2,"ECM") there are three CDC-ACM interfaces for AT commands and data, hence at most three dial-up connections can be established. In the “Fairly back-compatible Profile” (AT+UUSBCONF=0) there are six CDC-ACM interfaces, but only the three of them are available for AT commands and data, therefore at most three dial-up connections can be established.

A PPP dial-up connection can be started on an already active PDP context/EPS bearer only when the module is in the “Fairly back-compatible Profile” (USB profile defined with AT+UUSBCONF=0). In the case of the LTE networks, this implies that the initial default EPS bearer, which is always established at the time of attachment to the LTE network, is suitable for dial-up connections on the module. Also note that the already active PDP context/EPS bearer should be provided with the network/internet connectivity so that the PPP also has the connectivity. In this case the activation of a PPP session over an already active CID will move to connectivity for the previous configuration to the PPP session. Depending on the network provider policy for LTE networks, the cellular connectivity configuration requests the use of the +UCGDFLT AT command.

⚠ A dial-up acquires exclusive access to a PDP context: therefore it should be noted that activating a PPP session over an already active CID will disrupt connectivity for the previous user (if present).

The following example refers to an attempt of dial-up connection when the module attached to a 4G network:

1. The module is in router mode.
2. The module is in “Fairly back-compatible Profile” and it has +UCGDFLT’s APN configured for internet connectivity.
3. The cellular module IP subsystem is configured to access the internet through the cellular network within an internal context.
4. The module registers on a LTE network: the initial PDP context is activated on CID 4.
5. The initial PDP context is providing connectivity for the cellular module IP subsystem.
6. The dial-up session is started over the already active CID 4:
   - The PPP session now has exclusive access to the initial PDP connectivity;
   - The cellular module IP subsystem has no access to the internet and it must be reconfigured to use a different PDP context (if possible).

7. To give internet connectivity to both PPP and IP subsystem through the cellular network, two PDP contexts must be used.

In addition, also a further example is provided for the case of the module attached to a 2G/3G network:

1. The module is in router mode.
2. The module is in “Fairly back-compatible Profile” and it is attached to a 2G/3G network.
3. The module IP subsystem is configured to access the internet through the cellular network within an internal context (defined and activated).
4. The active PDP context is providing connectivity for the module IP subsystem.
5. The dial-up session is started over the already active context:
   - The PPP session now has exclusive access to the initial PDP connectivity;
   - The module IP subsystem has no access to the internet and it must be reconfigured to use a different PDP context (if possible).
6. To give internet connectivity to both PPP and module IP subsystem through the cellular network, two PDP contexts must be used.

Figure 8 shows the dial-up connection in bridge mode and “Low/Medium Throughput Profile”, while Figure 9 shows the coexistence between one dial-up connection and two active PDP context/EPS bearer when “Fairly back-compatible Profile” is active.

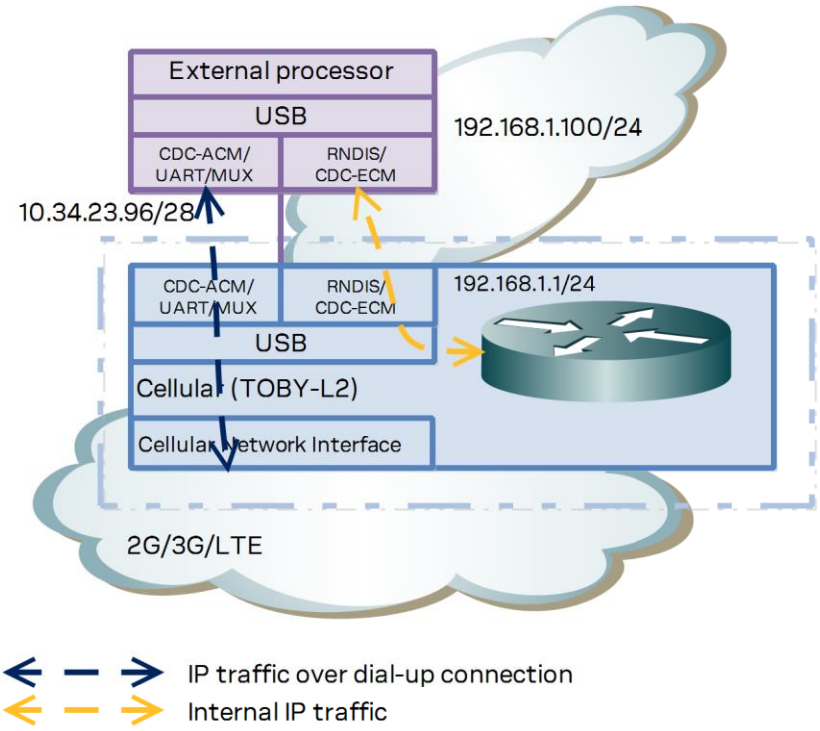


Figure 8: Single PDP context with PPP (bridge mode)

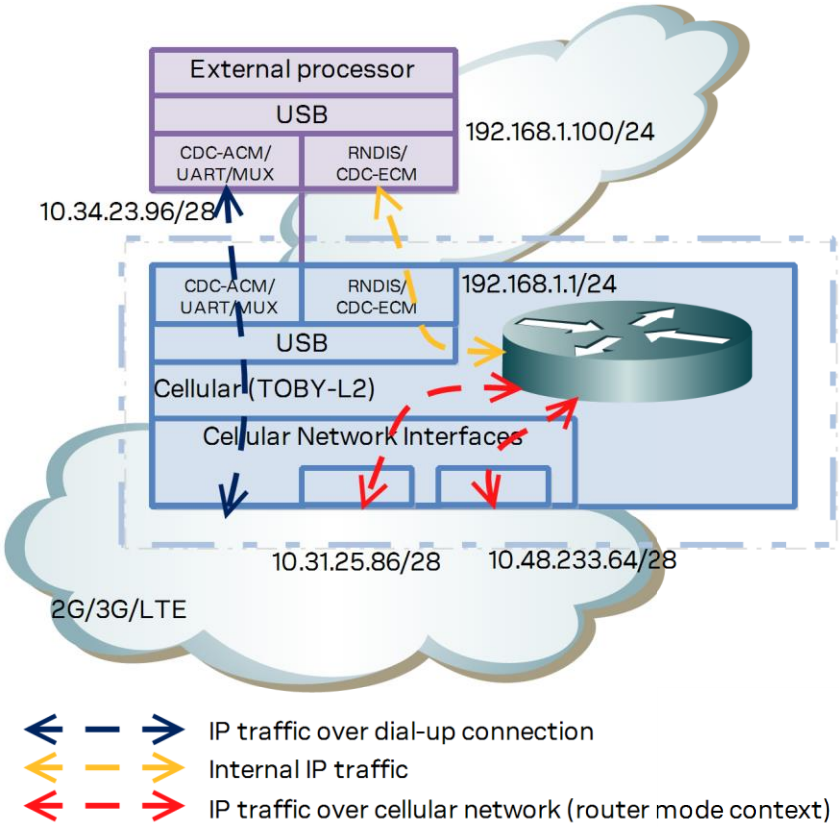


Figure 9: 3 PDP contexts, one PPP (router mode)

4.2.1 Dial-up PPP configuration on Linux systems

On Linux platforms the PPP connection shall be established with “wvdial”, which is a text-based dial-up application. The following configuration script shall be used to activate a PPP connection on the CID number <cid>.

```
[Dialer Defaults]
Modem Type = USB Modem
ISDN = 0
Init1 = ATZ
Init2 = AT+CGDCONT=<cid>,"IP",<apn>
Modem = /dev/ttyACM<X>
Baud = 460800
Phone = *99***<cid>#
; Username = <Login Name>
; Password = <Password>
```

In the script, <cid> represents the context identifier on which the PPP connection should be activated, <apn> is the APN name of the configured context, and /dev/ttyACM<X> represents the name of the device recognized by the system. Some mobile operators could also request a login name and a password, <Login Name> and <Password> respectively. The semicolon, indicating that the line is a comment, should be removed to specify the login and password parameters.

The application “wvdial” can be run with superuser privileges with the command `wvdial`.

4.2.2 Dial-up PPP configuration on Windows systems

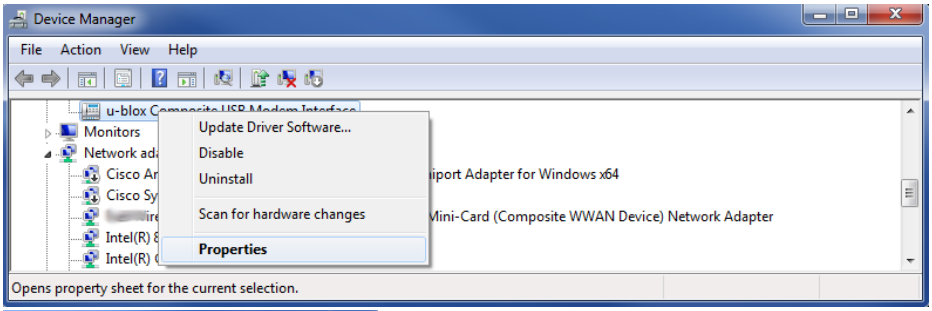
On Windows systems, a new dial-up connection should be configured via the menu:

Start > Control Panel > Network and Sharing Center > Set up a new connection or network

The configuration procedure requires the selection of the target (modem device) and the number to dial. On Windows systems the configuration of the context should be performed manually via AT command or through Windows modem properties. For example, to set the APN name on context 1 the user should specify the AT command:

```
at+cgdcont=1,"IP","<apn>"
```

The final result of the configuration is shown in the following figures:



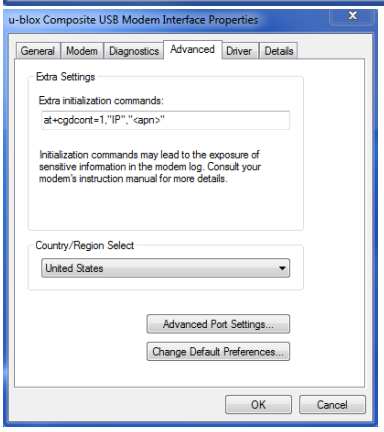


Figure 10: Dial-up Connection Windows

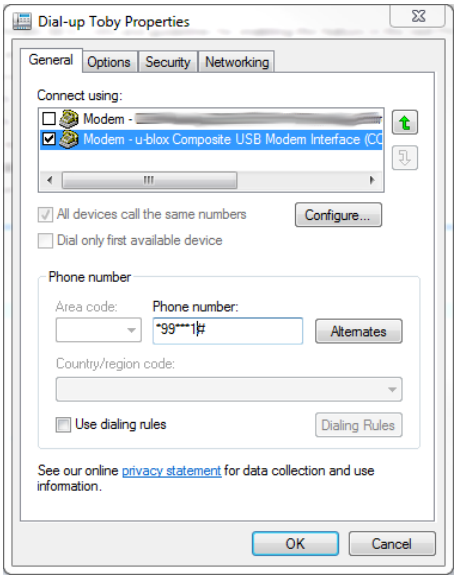


Figure 11: Properties > General tab

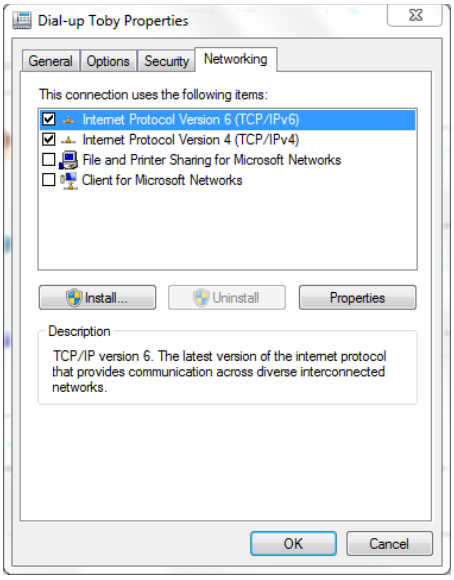


Figure 12: Properties > Networking tab

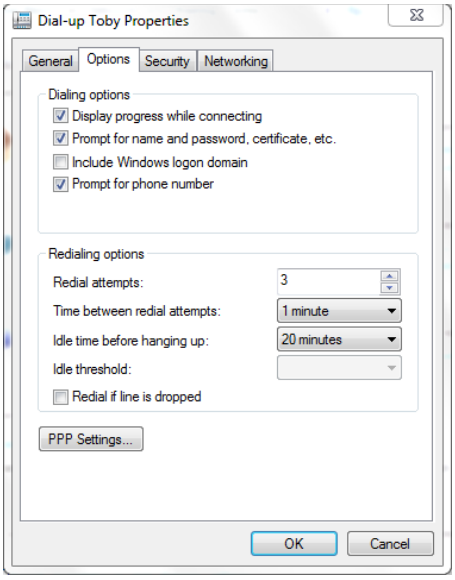


Figure 13: Properties > Options tab

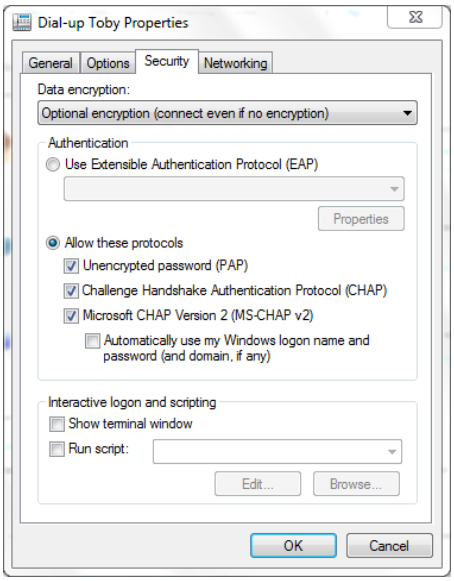


Figure 14: Properties > Security tab

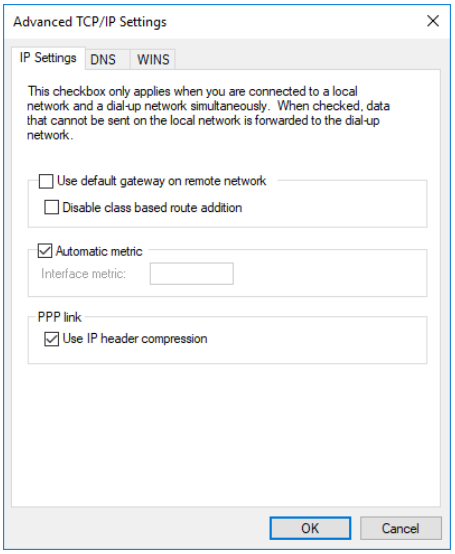


Figure 15 Default gateway within dial-up connection

In Figure 15 the selection of the “Use default gateway on remote network” option allows the user to set the default gateway within the dial-up connection. When this option is not enabled, the routing table of the DTE will not be modified.

4.3 Local dial-up connection

☞ The local dial-up is not supported by TOBY-L2 and MPCI-L2 "00S" / "50S" product versions.

u-blox cellular modules support the local dial-up connection. This feature allows modules to establish an IP-based connection with an external application processor through CDC-ACM, UART or MUX interfaces. During the local dial-up, a point to point connection is created between the module IP stack and the external application processor IP stack. The established connection is denoted by two IP addresses belonging to the same private subnetwork. Two IP addresses are required, one for each ending of the dial-up connection. The subnetwork, defined for the local dial-up, should be different from the subnetworks used for RNDIS/CDC-ECM interfaces. The local dial-up assigns to the host also the DNS server IP address. The IP address of the specified DNS server is equal to the local dial-up IP address of the target. In this configuration the target is performing as the DNS server for the host. If a different DNS server is requested, it should be defined by the customer during the IP network configuration of the host. Figure 16 shows the IP connections when the local dial-up feature is enabled on one MUX interface.

The local dial-up feature can be used when:

- the external processor does not have an RNDIS/CDC-ECM interface, and it is provided with an IP stack
- the IP connectivity between the UART and RNDIS/CDC-ECM interfaces is requested
- only one PDP context/EPS bearer shall be used to provide internet connectivity to the external processor through the UART or RNDIS/CDC-ECM interfaces

The `ATD*99***100#` command activates the local dial-up feature. The CID number 100 does not conflict with the CIDs used for dial-up connections, which are related to PDP contexts/EPS bearers.

☞ The local dial-up creates a subnetwork with a fixed IP range: 192.168.10.1/30.

Follow these operations to obtain the internet connectivity on the external processor through two MUX interfaces:

1. activate two MUX interfaces on UART
2. activate the local PPP on one of the virtual port by sending the `ATD*99***100#` command
3. use the second virtual ports for sending AT commands
4. activate one PDP context (+CGDCONT, +CGACT) or use the EPS bearer (+UCGDFLT):
   - if after boot the module is registered on 4G network, check that the default bearer has IP connectivity, if not, configure the APN with +UCGDFLT
   - if after boot the module is registered on 3G or 2G network, define a PDP context (+CGDCONT) and activate it (+CGACT)

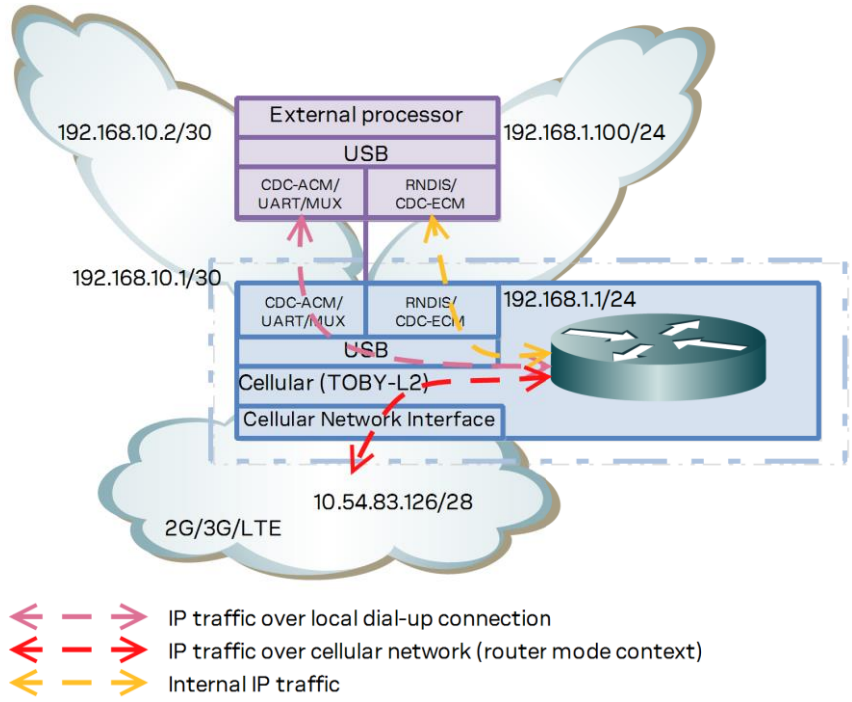


Figure 16: Local dial-up connection on one MUX interface in router mode

4.3.1 Conflicts between RNDIS/CDC-ECM private network and local dial-up connection

Since the IP configuration of the local dial-up is fixed (192.168.10.1/192.168.10.2), it shall not conflict with IP configuration of the USB virtual Ethernet interface (RNDIS/CDC-ECM). This may lead to an incorrect routing configuration.

To avoid loss of connectivity, the module should be properly configured:

Command	Response	Description
`AT+UIPCONF?`	`+UIPCONF: "192.168.10.1","255.255.255.0","192.168.10.100","192.168.10.100","FE80::2C60:21FF:FC56:2A2A/64"` `OK`	Retrieve the network configuration on the module USB virtual Ethernet interface. The conflict between the RNDIS/CDC-ECM connection and local dial-up connection is present. The IP configuration of the RNDIS/CDC-ECM interface shall not include IP addresses in the range192.168.10.1-192.168.10.3.

Command	Response	Description
AT+UIPCONF="192.168.254.1","255.255.255.0","192.168.254.100","192.168.254.100"	OK	The IP network configuration of the RNDIS/CDC-ECM shall be adjusted to provide a new IP address/mask and a new range for the DHCP server running on the USB virtual Ethernet interface.
AT+CFUN=1,1	OK	Finally, the module should be rebooted to make effective the applied changes. It is worth noticing that also the host IP network configuration shall be verified and when needed adjusted (especially in the case of static addressing).
AT+UIPCONF="192.168.10.4","255.255.255.0","192.168.10.100","192.168.10.100"	OK	In case the subnetwork 192.168.10.0/24 is needed, the first available IP address is 192.168.10.4/24.

4.4 Multiple PDP contexts/EPS bearers

In LTE, PS data connections are referred to as EPS bearers: EPS bearers are conceptually equivalent to the legacy PDP contexts, which are often referred to for the sake of simplicity.

Similarly to a PDP context, the EPS bearer can be a default (primary) or dedicated (secondary) one. The initial EPS bearer established during LTE Attach procedure is actually a default EPS bearer.

When attached to an LTE network with some mobile operators, it may occur that the activation of user-defined EPS default bearers is rejected by the network. In this case the connectivity may be granted by the default initial EPS bearer when it is configured as an initial PDP context (+UCGDFLT AT command) and using the module in route mode through the RNDIS interface. Using the module in the “Fairly back-compatible Profile”, a PPP connection may be performed on an active default initial EPS bearer configured as an initial PDP context.

Check the user-defined EPS bearers availability with the current mobile network operator.

If the initial default EPS bearer is not suitable for internet connectivity, like on Verizon network where is it devoted to IMS services, activate a second default EPS bearer with appropriate APN to enable PS data services. This can be automatically done by the module on Verizon network (see +UMNOCONF AT command). In Verizon configuration, if the IMS APN gives no IP/IPv6 connectivity or the LTE attach fails, then the module will automatically select the internet APN and perform the LTE attach with it.

4.4.1 Module cellular connectivity in relation to USB interface profile and networking mode

The module is able to handle a maximum of eight contexts. However, the context configuration depends on the USB interface profile and on the networking modes.

As reported in section 4.1.6, the module offers three USB interface profiles: a fairly backwards-compatible profile, a low/medium throughput profile and a high throughput profile. In the first USB profile there are six CDC-ACM interfaces, but only three of them can be used for connectivity purposes. The second profile provides three CDC-ACM interfaces (all of them can be used for connectivity purposes) and one CDC-ECM interface. The last profile offers only one CDC-ACM interface and one RNDIS interface.

u-blox cellular modules can operate in two different networking modes: router and bridge mode. The complete description is provided in sections 2 and 3. The context configuration is done accordingly to the networking mode.

Furthermore, when the module is in bridge mode, the contexts can be reconfigured as router contexts by means of the command +UDPDP. In this case the target becomes the context's owner to have internal connectivity.

In both networking modes, the PPP connections are one-to-one to the number of available CDC-ACM interfaces used for connectivity purposes.

☞ Besides the CDC-ACM interfaces, the AT command interface or a PPP connection can be established on the UART/MUX interfaces (this topic is out of scope for this application note).

Table 1 summarizes the configuration of the PDP contexts in relation to the USB profile and the networking mode.

		Router mode (AT+UBMCONF=1)		Bridge mode (AT+UBMCONF=2)	
Fairly back-compatible profile (AT+UUSBCONF=0)	6 CDC-ACM (only 3 of 6 are for connectivity purposes)	R=1:R_{max} P=1:P_{max} A=R+P	R_{max}=8* P_{max}=3 A_{max}=8	R=1:R_{max} P=1:P_{max} A=R+P	R_{max}=8* P_{max}=3 A_{max}=8
Low/Medium throughput profile (AT+UUSBCONF=2)	3 CDC-ACM 1 CDC-ECM	R=1:R_{max} P=1:P_{max} A=R+P	R_{max}=8 P_{max}=3 A_{max}=8	R=1:R_{max} P=1:P_{max} B=1:B_{max} A=R+P+B	R_{max}=8* P_{max}=3 B_{max}=8 A_{max}=8
High throughput profile (AT+UUSBCONF=3)	1 CDC-ACM 1 RNDIS	R=1:R_{max} P=1:P_{max} A=R+P	R_{max}=8 P_{max}=1 A_{max}=8	R=1:R_{max} P=1:P_{max} B=1:B_{max} A=R+P+B	R_{max}=8* P_{max}=1 B_{max}=8 A_{max}=8
Low/Medium throughput profile (AT+UUSBCONF=12)	2 CDC-ACM 1 SAP port 1 CDC-ECM	R=1:R_{max} P=1:P_{max} A=R+P	R_{max}=8 P_{max}=2 A_{max}=8	R=1:R_{max} P=1:P_{max} B=1:B_{max} A=R+P+B	R_{max}=8* P_{max}=2 B_{max}=8 A_{max}=8
High throughput profile (AT+UUSBCONF=13)	1 SAP port 1 RNDIS	R=1:Rmax P=1:Pmax A=R+P	R_{max}=8 P_{max}=0 Amax=8	R=1:R_{max} P=1:P_{max} B=1:B_{max} A=R+P+B	R_{max}=8* P_{max}=0 B_{max}=8 Amax=8

Table 1: Contexts configuration in relation to the USB profile and the networking mode

where:

- R = router context
- R_{max} = maximum number of router contexts
- P = PPP session (one to one to CDC-ACM interface)
- P_{max} = maximum number of PPP sessions
- B = bridge context
- B_{max} = maximum number of bridge contexts
- A = total number of contexts
- A_{max} = maximum number of contexts
- * = the contexts are ONLY available to the target

Appendix

A IP subsystem configuration

This appendix provides the most important shell commands needed to configure the IP subsystem of a generic Windows and Linux operating system.

This convention used in the following IPv4 examples is:

- A1.A2.A3.A4 denotes an IPv4 address
- abcX is the name of the interface in a Linux OS
- Y is the number of the virtual interface in Linux OS
- G1.G2.G3.G4 is the IPv4 gateway
- N1.N2.N3.N4/M denotes an IPv4 subnetwork
- M is the size of the IPv4 subnetwork bit field
- M1.M2.M3.M4 is the mask in dotted decimal notation
- Ifname is the name of the interface under Windows
- Ifnum is the number of the interface under Windows
- and DNS1 is the IPv4 address of the DNS server in dotted-decimal notation

Moreover, the IPv6 address is 128 bit long and it is subdivided in 64-bit prefix (PREFIX_64) and 64-bit suffix (SUFFIX_64). Each network device has its local IPv6 address, which typically looks like FE80::SUFFIX_64, where FE80::/64 is the link local prefix (LINKLOCAL_64). Each network interface sends a Router Solicitation message to find the next hop router. The next hop router will reply with a Router Advertisement message. The Router Advertisement message will contain the PREFIX_64, which is used by the network interface to define its global IPv6 address (PREFIX_64:SUFFIX_64). The IPv6 gateway will have the GW_PREFIX_64:GW_SUFFIX_64 address, while IPv6_SUBNET denotes a specific IPv6 subnetwork.

A.1 IPv4 interface configuration in Windows OS

ID	DOS command	Explanation
1	`netsh int ip add address name="Ifname" addr=A1.A2.A3.A4 mask= M1.M2.M3.M4`	Set the IP address of the interface Ifname and of the virtual interface of Ifname
2	`netsh int ip del address name="Ifname" addr=A1.A2.A3.A4`	Unset the IP address of the interface Ifname and of the virtual interface of Ifname
3	`route ADD 0.0.0.0 MASK M1.M2.M3.M4 G1.G2.G3.G4 METRIC 1 IF Ifnum`	Set default gateway
4	`route DELETE 0.0.0.0 G1.G2.G3.G4`	Unset the default gateway
5	`route ADD N1.N2.N3.N4 MASK M1.M2.M3.M4 G1.G2.G3.G4 IF Ifnum`	Set a gateway for a specific network
6	`route DELETE N1.N2.N3.N4`	Unset a gateway for a specific network
7	`netsh int ip add dns name="Ifname" addr=DNS1`	Set a DNS server
8	`netsh int ip del dns name="Ifname" addr=DNS1`	Unset a DNS server

A.2 IPv4 interface configuration in Linux OS

ID	Bash command	Explanation
1	`ifconfig abcX A1.A2.A3.A4`	Set the IP address of the interface abcX

2	`ifconfig abcX:Y A1.A2.A3.A4 netmask M1.M2.M3.M4 pointopoint G1.G2.G3.G4 up`
	or
	`ip addr add A1.A2.A3.A4/M peer G1.G2.G3.G4 dev abcX`
		Set the IP address of the virtual interface Y of abcX (in bridge mode see the note how to obtain gateway address). The keywords "pointopoinit" and "peer" enables the point-to-point mode of an interface, meaning that it is a direct link between two machines with nobody else listening on it

3	`route add default gw G1.G2.G3.G4`	Set default gateway
4	`route del default`	Unset the default gateway
5	`route add -net N1.N2.N3.N4/M gw G1.G2.G3.G4`	Set a gateway for a specific network
6	`route del -net N1.N2.N3.N4/M gw G1.G2.G3.G4`	Unset a gateway for a specific network
7	`echo "nameserver DNS1" >> /etc/resolv.conf`	Set a DNS server

A.3 IPv6 interface configuration in Windows OS

ID	DOS command	Explanation
1	`netsh interface ipv6 add address "Ifname"LINKLOCAL_64:SUFFIX_64`	Set the IPv6 link local address of the interface Ifname
2	`netsh interface ipv6 add address "Ifname" PREFIX_64:SUFFIX_64`	Set the IPv6 global address of the interface Ifname
3	`netsh interface ipv6 del address "Ifname" LINKLOCAL_64:SUFFIX_64`	Unset the IPv6 link local address of the interface Ifname
4	`netsh interface ipv6 del address "Ifname" PREFIX_64:SUFFIX_64`	Unset the IPv6 global address of the interface Ifname
5	`netsh interface ipv6 add route IPv6_SUBNET "Ifname" GW_PREFIX_64:GW_SUFFIX_64`	Set gateway on the interface Ifname for subnetwork IPv6_SUBNET
6	`netsh interface ipv6 del route IPv6_SUBNET "Ifname" GW_PREFIX_64:GW_SUFFIX_64`	Unset gateway on the interface Ifname for subnetwork IPv6_SUBNET
7	`netsh interface ipv6 add dnsserver "Ifname" DNS-IPv6`	Set a DNS server on the interface Ifname
8	`netsh interface ipv6 del dnsserver "Ifname" DNS-IPv6`	Unset a DNS server on the interface Ifname
9	`netsh interface ipv6 add neighbors "Ifname" RANDOM-SUFFIX_64`	Prevent Neighbor Discovery on the interface Ifname, by adding a neighbor with a random IPv6 address
10	`netsh int ipv6 set privacy state=disabled/enabled`	Disable/enable IPv6 privacy extensions. Used with example ID 11.
11	`netsh interface ipv6 set global randomizeidentifiers=disabled store=active` `netsh interface ipv6 set global randomizeidentifiers=disabled store=persistent`	Disable random generation for non-temporary autoconfigured IPv6 addresses. The IPv6 addresses are based on IEEE EUI-64
12	`netsh int ipv6 set interface "Ifname" routerdiscovery=disabled/enabled`	Disable/enable sending Router Solicitation
13	`netsh int ipv6 set interface "Ifname" advertise=disabled/enabled`	Disable/enable sending Router Advertisement

☞ With the netsh option `store=active` the changes are applied for the current session, while with the option `store=persistent` the changes are applied permanently.

A.4 IPv6 interface configuration in Linux OS

ID	Bash command	Explanation
1	`ip -6 addr add LINKLOCAL_64:SUFFIX_64 dev abcX`	Set the IPv6 link local address of the interface abcX
2	`ip -6 addr add PREFIX_64:SUFFIX_64 dev abcX`	Set the IPv6 global address of the interface abcX
3	`ip -6 addr del LINKLOCAL_64:SUFFIX_64 dev abcX`	Unset the IPv6 link local address of the interface abcX
4	`ip -6 addr del PREFIX_64:SUFFIX_64 dev abcX`	Unset the IPv6 global address of the interface abcX
5	`ip -6 route add IPv6_SUBNET via GW_PREFIX_64:GW_SUFFIX_64`	Set gateway on the interface abcX
6	`ip -6 route del IPv6_SUBNET via GW_PREFIX_64:GW_SUFFIX_64`	Unset default gateway on the interface abcX
7	`echo "nameserver DNS-IPv6" >> /etc/resolv.conf`	Set a DNS server
8	`delete the related row from the file /etc/resolv.conf`	Unset a DNS
9	`ip neigh add GW_PREFIX_64:RANDOM_SUFFIX_64 lladdr RANDOM_MAC_ADDR dev abcX`	In bridge mode on host side: prevent Neighbor Discovery on the interface abcX, by adding a fictitious neighbor with a random IPv6 address
10	`ip neigh del GW_PREFIX_64:RANDOM_SUFFIX_64 lladdr RANDOM_MAC_ADDR dev abcX`	In bridge mode on host side: delete the fictitious neighbor associated with the interface abcX
11	`ip neigh show`	In bridge mode on host side: show the list of the neighbor
12	`In /etc/radvd.conf: AdvSendAdvert off|on`	Disable / enable sending Router Advertisement and Router Solicitation.
13	`sudo sysctl -w net.ipv6.conf.all(abcX).autoconf=0`	Autoconfigure addresses using prefix information from router advertisements.
14	`sudo sysctl -w net.ipv6.conf.all(abcX).use_tempaddr=<value>`	Disable random generation for non-temporary autoconfigured IPv6 addresses. The IPv6 addresses are based on IEEE EUI-64. This option disable/enable IPv6 privacy extensions. `<value>` can be chosen from the following: ☞ <=0 Disable Privacy Extensions (i.e. do not use changing temporary addresses at all). ☞ ==1 Use the Privacy Extensions, but prefer public (i.e. non-temporary) addresses over temporary ones. ☞ >1 (e.g. 2 as here) Use the Privacy Extensions and prefer them.

☞ In the sysctl commands, “all” stands for all interfaces, while “abcX” stands for only for the abcX interface.

B Router/bridge mode configuration in Linux

The example setup has been performed on a Linux machine running Ubuntu 14.04 distribution.

In **Router mode** the following setting shall be used in Linux:

- Open a terminal
- Identify the interface associated with the USB virtual Ethernet (i.e. usb1)
- Input `ifconfig`, the RNDIS is not active yet
- Input `dhclient usb1` to configure the DHCP client, now the USB virtual Ethernet interface is active
- Input `ifconfig` and check that USB virtual Ethernet is active

In **Bridge mode** the following setting shall be used in Linux:

- Precondition: a data context is already active on the module
- For example 100.87.53.78 is the IP address obtained with +CGDCONT (or + CGCONTRDP), usb1 is the interface associated to RNDIS and 100.87.53.177 is the virtual IP that is obtained with +UIPADDR
- Open a terminal
- Input `killall dhclient`
- Input `ifconfig usb1 192.168.1.149 netmask 255.255.255.0`
- `ping 192.168.1.1` (it is possible to ping the module and for tracing purposes)
- `ping 8.8.8.8` (it will return an error because the routing rules are missing)
- `ifconfig usb1:0 100.87.53.78 netmask 255.255.255.255 pointopoint 100.87.53.177 up` (similar to 'alias' in Windows, 'pointopoint' sets up a two hosts network with the module)
- `ping 8.8.8.8` (it will return an error because we need to specify how to route the traffic)
- `route add default gw 100.87.53.177`
- `ping 8.8.8.8` (it is possible to ping an external address)
- `ifconfig usb1 down` (it closes the RNDIS interface)

C How to use multiple PDP contexts in router/bridge mode

This section provides an example about how to use multiple PDP contexts (at least two) and how to subdivide the IP traffic between them. The example is provided for Windows and Linux operating systems, and for the cellular module in router and bridge mode.

C.1 Router mode

The test can be subdivided into two parts. The first part of the setup is different for GSM/UMTS networks and LTE networks. The second part is common to both cases.

Part for GSM/UMTS networks:

- Ensure that the module is registered with a GSM/UMTS network
- Define two PDP contexts with the +CGDCONT AT command
- Activate the first defined PDP context with +CGACT AT command
- Activate the second defined PDP context

Part for LTE networks:

- Ensure that the module has connectivity on the initial default bearer in LTE network
- Define the second default bearer with the +CGDCONT AT command
- Activate the second defined PDP context

Common part:

- Check which IP address is used (use +CGDCONT and Internet browser)
- Set which host should be reached through the second PDP context
- Check if the previous step has been successful

☞ On TOBY-L2 "03" product versions (except for TOBY-L200-03S-00, TOBY-L210-03A-00, TOBY-L210-03S-00, TOBY-L280-03S-00), to prevent missing the resolution of URLs within private DNS servers it is suggested to define the routing rules to reach the private DNS servers accordingly. This operation is not necessary, when the private DNS servers are reachable through the default gateway. However, in multiple PDP context scenarios the default gateway may change.

The example is valid for both Linux and Windows OS, since Internet browser and ping application are available in both of them.

Part for GSM/UMTS networks:

Command	Response	Description
AT+UBMCONF?	+UBMCONF: 1 OK	Check that the module is in router mode. If not, set it accordingly.
AT+COPS?	+COPS: 0,0,"vodafone IT",2 OK	Check that the module is registered on a GSM/UMTS network. If the module is not registered on a UMTS network, use the +URAT AT command to lock the module to the specified radio access technology.
AT+CGDCONT=1,"IP","web.omnitel.it"	OK	Define the first PDP context with the proper APN (CID= 1).
AT+CGDCONT=2,"IP","web.omnitel.it"	OK	Define the second PDP context with the proper APN (CID= 2).
AT+CGDCONT?	+CGDCONT: 1,"IP","web.omnitel.it","",0,0,0,0,0,0 +CGDCONT: 2,"IP","web.omnitel.it","",0,0,0,0,0,0 OK	The two PDP contexts are defined but not enabled.
AT+CGACT=1,2	OK	Activate the first PDP context (CID=2).
AT+CGDCONT?	+CGDCONT: 1,"IP","web.omnitel.it","",0,0,0,0,0,0 +CGDCONT: 2,"IP","web.omnitel.it","37.177.70.238",0,0,0,0,0,0 OK	Check the IP address ("37.177.70.238") associated to the PDP context (CID=2). In router mode it is worth noticing that: • activating only one PDP context all the IP traffic is forwarded through it (it is used as the default gateway)
AT+CGACT=1,1	OK	Activate the second PDP context (CID=1).
AT+CGDCONT?	+CGDCONT: 1,"IP","web.omnitel.it","37.177.17.125",0,0,0,0,0,0 +CGDCONT: 2,"IP","web.omnitel.it","37.177.70.238",0,0,0,0,0,0 OK	Check the IP addresses ("37.177.70.238" for CID=2 and "37.177.17.125" for CID=1) associated to the two PDP contexts. In router mode it is worth noticing that: • for multiple active contexts the default gateway is associated to the oldest active PDP context (in this case CID=2)

Part for LTE networks:

Command	Response	Description
AT+UBMCONF?	+UBMCONF: 1 OK	Check that the module is in router mode. If not, set it accordingly.
AT+COPS?	+COPS: 0,0,"vodafone IT",7 OK	Check that the module is registered on a 4G network. If the module is not registered on a 4G network, use the +URAT AT command to lock the module to the specified radio access technology.
AT+CGDCONT?	+CGDCONT: 4,"IP","ims.mnc010.mcc222.gprs","93.68.170.89",0,0,0,0,0,0 OK	Check if there is connectivity on the initial default bearer. In this case the internet connectivity is not available, hence next 3 step should be performed.
AT+CFUN=4	OK	Set the module in airplane mode to configure the default PDP context for LTE network.
AT+UCGDFLT=1,"IP",web.omnitel.it"	OK	Configure the initial PDP context for LTE network.
AT+CFUN=1	OK	Sets the MT to full functionality.
AT+CGDCONT?	+CGDCONT: 4,"IP","web.omnitel.it.mnc010.mcc222.gprs","37.177.70.238",0,0,0,0,0,0 OK	Check if there is connectivity on the initial default bearer. In this case the internet connectivity is available. In router mode it is worth noticing that: • Since the initial default bearer is the first activated context, it is used as the default gateway.
AT+CGDCONT=1,"IP","mobile.vodafone.it"	OK	Define the second PDP context with the proper APN (CID=1). ☞ On several 4G network only one APN can be associated to single context.
AT+CGACT=1,1	OK	Activate the second PDP context (CID=1).
AT+CGDCONT?	+CGDCONT: 1,"IP","mobile.vodafone.it.mnc010.mcc222.gprs","37.177.17.125",0,0,0,0,0,0 +CGDCONT: 4,"IP","web.omnitel.it.mnc010.mcc222.gprs","37.177.70.238",0,0,0,0,0,0 OK	Check the IP addresses ("37.177.70.238" for CID=4 and "37.177.17.125" for CID=1) associated to the PDP context. In router mode it is worth noticing that: • For multiple active contexts the default gateway is associated to the oldest active PDP context (in this case CID=4).

Common part:

Command	Response	Description
AT+UIPADDR=1	+UIPADDR: 1,"ccinet0","37.177.17.125","255.255.255.255","","" OK	Get the configuration of the active PDP IPv4 only context/EPS bearer with CID=1.
AT+UIPROUTE="add -net 93.184.219.82 netmask 255.255.255.255 dev ccinet0"	OK	In router mode the +UIPROUTE AT command should be used to define which PDP context should be used to reach the defined host. In this case the IP address of the host is 93.184.219.82 (www.speedtest.net) and it is configured to be reachable via the second PDP context (ccinet0).
AT+UIPROUTE="add -host www.speedtest.net dev ccinet0"	OK	Command equivalent to the previous one.

DNS servers routing rules for GSM/UMTS networks (optional, valid for TOBY-L2 "03" product versions):

Command	Response	Description
AT+CGCONTRDP=1	+CGCONTRDP: 1,6,"web.omnitel.it","37.177.17.125.255.255.255.255","37.177.17.125","10.133.11.210","83.224.65.106","0.0.0.0","0.0.0.0",0 OK	Check the IP configuration of the second PDP context (CID=1).
AT+CGCONTRDP=2	+CGCONTRDP: 2,6,"web.omnitel.it","37.177.70.238.255.255.255.255","37.177.70.238","10.133.13.210","10.132.100.181","0.0.0.0","0.0.0.0",0 OK	Check the IP configuration of the first PDP context (CID=2).
AT+UIPROUTE="add -host 10.133.11.210 gw 37.177.17.125"	OK	Set the route for the DNS1 server within the second context.
AT+UIPROUTE="add -host 83.224.65.106 gw 37.177.17.125"	OK	Set the route for the DNS2 server within the second context.
AT+UIPROUTE="add -host 10.133.13.210 gw 37.177.70.238"	OK	Set the route for the DNS1 server within the first context.
AT+UIPROUTE="add -host 10.132.100.181 gw 37.177.70.238"	OK	Set the route for the DNS2 server within the first context.

DNS servers routing rules for LTE networks (optional, valid for TOBY-L2 "03" product versions):

Command	Response	Description
AT+CGCONTRDP=1	+CGCONTRDP: 1,6,"web.omnitel.it","37.177.17.125.255.255.255.255","37.177.17.125","10.133.11.210","83.224.65.106","0.0.0.0","0.0.0.0",0 OK	Check that IP configuration of the second PDP context (CID=1).
AT+CGCONTRDP=4	+CGCONTRDP: 4,6,"web.omnitel.it","37.177.70.238.255.255.255.255","37.177.70.238","10.133.13.210","10.132.100.181","0.0.0.0","0.0.0.0",0 OK	Check that IP configuration of the first PDP context (CID=4).
AT+UIPROUTE="add -host 10.133.13.210 gw 37.177.70.238"	OK	Set the route for the DNS1 server within the second context.
AT+UIPROUTE="add -host 10.132.100.181 gw 37.177.70.238"	OK	Set the route for the DNS2 server within the second context.
AT+UIPROUTE="add -host 10.133.11.210 gw 37.177.17.125"	OK	Set the route for the DNS1 server within the first context.
AT+UIPROUTE="add -host 83.224.65.106 gw 37.177.17.125"	OK	Set the route for the DNS2 server within the first context.

As a proof of the validity of the configuration:

- Open a browser and go to the address www.speedtest.net
- In the bottom left angle of the page, the IP of the second defined PDP context will be reported

The displayed IP corresponds to the IP associated to the second context because the traffic to the host www.speedtest.net is forwarded within the second PDP context.

- As a countercheck, open a browser on a page displaying the IP address (like www.whatismyip.com): the displayed IP address corresponds to the IP associated to the first PDP context, which is used as default gateway that is “37.177.70.238”.

C.2 Bridge mode

The test is related to the use of GSM/UMTS/LTE networks, and can be subdivided in the following steps. The first part of the setup is different for GSM/UMTS networks and LTE networks. The second part is common to both cases.

Part for GSM/UMTS networks:

- Ensure that the module is registered on a 2G/3G network
- Define the first PDP context with the +CGDCONT AT command
- Activate the first defined PDP context with +CGACT AT command
- Check which IP address is used for the first PDP context (use +CGDCONT and Internet browser)
- Define the second PDP context with the +CGDCONT AT command

Part for 4G networks:

- Ensure that the module has connectivity on the initial default bearer in 4G network
- Check which IP address is used for the first PDP context (use +CGDCONT and Internet browser)
- Define the second default bearer with the +CGDCONT AT command

Common part:

- Define the IP address alias for the first defined PDP context
- Activate the second defined PDP context
- Check which IP address is used (use +CGDCONT and Internet browser)
- Define the IP address alias for the second defined PDP context
- (for debug purposes) Retrieve the IP configuration of the module RNDIS/CDC-ECM interface using the +UIPCONF AT command. Define the IP address alias compliant with IP configuration of the module RNDIS/CDC-ECM interface.
- Set which host should be reached through the second PDP context
- Check if the previous step has been successful

The presented example is valid for Linux and Windows operating systems, since Internet browser and ping application are available in both of them. The test sequence differs on Linux and Windows operating system, since the commands for the network interface configuration are different.

At the beginning of the test sequence check that the cellular module is in the proper networking mode by means of the +UBMCONF AT command. If the module is not in the right mode (router or bridge) the user should set the new mode and should reboot the module. After the reboot the following steps can be performed:

Part for GSM/UMTS networks:

Command	Response	Description
AT+UBMCONF?	+UBMCONF: 2 OK	Check that the module is in bridge mode. If not, set it accordingly.
AT+COPS?	+COPS: 0,0,"vodafone IT",2 OK	Check that the module is registered on a 2G/3G network. If the module is not registered on a 3G network, use the +URAT AT command to lock the module to the specified radio access technology.
AT+CGDCONT=2,"IP","web.omnitel.it"	OK	Define the first PDP context with the proper APN (CID=1).
AT+CGDCONT?	+CGDCONT: 2,"IP","web.omnitel.it","",0,0,0,0,0,0 OK	The two PDP contexts are defined but not enabled.
AT+CGACT=1,2	OK	Activate the first PDP context (CID=2).
AT+CGDCONT?	+CGDCONT: 2,"IP","web.omnitel.it","37.177.70.238",0,0,0,0,0,0 OK	Check the IP address ("37.177.70.238") associated to the PDP context (CID=2).
AT+CGCONTRDP=2	+CGCONTRDP: 2,6,"web.omnitel.it","37.177.70.238.255.255.255.255","37.177.70.238","10.133.13.210","10.132.100.181","0.0.0.0","0.0.0.0",0 OK	Check that IP configuration of the first PDP context (CID=2).
AT+UIPADDR=2	+UIPADDR: 2,"usb0:1","37.177.70.17","255.255.255.0","","" OK	Get the IP address of the gateway for the first defined PDP context.
AT+CGDCONT=1,"IP","web.omnitel.it"	OK	Define the second PDP context with the proper APN (CID=2).

Part for 4G networks:

Command	Response	Description
AT+UBMCONF?	+UBMCONF: 2 OK	Check that the module is in bridge mode. If not, set it accordingly.
AT+COPS?	+COPS: 0,0,"vodafone IT",7 OK	Check that the module is registered on a 4G network. If the module is not registered on a 4G network, use the +URAT AT command to lock the module to the specified radio access technology.
AT+CGDCONT?	+CGDCONT: 4,"IP","ims.mnc010.mcc222.gprs","93.68.170.89",0,0,0,0,0,0 OK	Check if there is connectivity on the initial default bearer. In this case the internet connectivity is not available, hence next 3 step should be performed.
AT+CFUN=4	OK	Set the module in airplane mode to configure the default PDP context for LTE network.
AT+UCGDFLT=1,"IP",web.omnitel.it"	OK	Configure the initial PDP context for LTE network.
AT+CFUN=1	OK	Sets the MT to full functionality.
AT+CGDCONT?	+CGDCONT: 4,"IP","web.omnitel.it.mnc010.mcc222.gprs","37.177.70.238",0,0,0,0,0,0 OK	Check if there is connectivity on the initial default bearer. In this case the internet connectivity is available.
AT+CGCONTRDP=4	+CGCONTRDP: 4,6,"web.omnitel.it","37.177.70.238.255.255.255.255","37.177.70.238","10.133.13.210","10.132.100.181","0.0.0.0","0.0.0.0",0 OK	Check that IP configuration of the first PDP context (CID=2).
AT+UIPADDR=4	+UIPADDR: 4,"usb0:3","37.177.70.17","255.255.255.0","","" OK	Get the IP address of the gateway for the first defined PDP context.
AT+CGDCONT=1,"IP","mobile.vodafone.it"	OK	Define the second PDP context with the proper APN (CID=1). On several 4G network only one APN can be associated to single context.
AT+CGACT=1,1	OK	Activate the second PDP context (CID=1).

Common part:

Set interface for first context

On Windows OS execute the following commands:

```
> netsh int ip add address name="Ifname" addr=37.177.70.238 mask= 255.255.255.255
> route ADD 0.0.0.0 MASK 0.0.0.0 37.177.70.17 METRIC 1 IF Ifnum
> netsh int ip set dns name="Ifname" addr="10.133.13.210"
> netsh int ip set dns name="Ifname" addr="10.132.100.181" index=2
```

where Ifname and Ifnum are the name and the number of the RNDIS/CDC-ECM interface. Both the values can be recalled with the command:

```
> route PRINT
```

On Linux OS execute the following commands:

```
> ifconfig usb0:0 37.177.70.238 netmask 255.255.255.255 pointopoint 37.177.70.17 up
> route add default gw 37.177.70.17
> echo "namserver 10.133.13.210" >> /etc/resolv.conf
> echo "namserver 10.132.100.181" >> /etc/resolv.conf
```

where usb0 is the name of the RNDIS/CDC-ECM interface provided with the command:

```
> ifconfig
```

Open a browser on a page displaying your IP address (like www.whatismyip.com):

- the IP of the first defined PDP context is reported because the cellular network provider does not use IP masquerading on its network
- activating only one PDP context all the IP traffic is forwarded through it (it is used as the default gateway)
- in the cellular module the default gateway is associated to the oldest active PDP context

In GSM/UMTS networks:

Command	Response	Description
AT+CGCONTRDP=1	+CGCONTRDP: 1,6,"web.omnitel.it","37.177.17.125.255.255.255.255","37.177.17.125","10.133.11.210","83.224.65.106","0.0.0.0","0.0.0.0",0 OK	Check that IP configuration of the second PDP context (CID=1).

In LTE networks:

Command	Response	Description
AT+CGCONTRDP=1	+CGCONTRDP: 1,6,"mobile.vodafone.it.mnc010.mcc222.gprs","37.177.17.125.255.255.255.255","37.177.17.125","10.133.11.210","83.224.65.106","0.0.0.0","0.0.0.0",0 OK	Check that IP configuration of the second PDP context (CID=1).

Check which IP address that should be used as gateway for the second PDP context:

Command	Response	Description
AT+UIPADDR=1	+UIPADDR: 1,"usb0:0","37.177.17.130","255.255.255.0","","" OK	Get the IP address of the gateway for the second defined PDP context.

On Windows OS execute the following commands:

```
> netsh int ip add address name="Ifname" addr=37.177.17.125 mask= 255.255.255.255
> netsh int ip set dns name="Ifname" addr="10.133.11.210" index=3
> netsh int ip set dns name="Ifname" addr="83.224.65.106" index=4
```

where Ifname is the name of the RNDIS/CDC-ECM interface. This name can be recalled with the command:

```
> route PRINT
```

On Linux OS execute the following commands:

```
> ifconfig usb0:1 37.177.17.125 netmask 255.255.255.255 pointopoint 37.177.17.130 up
> echo " namserver 10.133.11.210" >> /etc/resolv.conf
> echo " namserver 83.224.65.106" >> /etc/resolv.conf
```

where usb0 is the name of the RNDIS/CDC-ECM interface provided with the command:

```
> ifconfig
```

☞ DNS servers routing rules (optional, valid for TOBY-L2 "03" product versions onwards except for TOBY-L200-03S-00, TOBY-L210-03A-00, TOBY-L210-03S-00, TOBY-L280-03S-00):

Set the routes the DNS servers within the proper PDP context

On Windows OS execute the following commands:

```
> route ADD 10.133.13.210 mask 255.255.255.255 37.177.70.17
> route ADD 10.132.100.181 mask 255.255.255.255 37.177.70.17
> route ADD 10.133.11.210 mask 255.255.255.255 37.177.17.130
> route ADD 83.224.65.106 mask 255.255.255.255 37.177.17.130
```

On Linux OS execute the following commands:

```
> route add -host 10.133.13.210 gw 37.177.70.17
> route add -host 10.132.100.181 gw 37.177.70.17
> route add -host 10.133.11.210 gw 37.177.17.130
> route add -host 83.224.65.106 gw 37.177.17.130
```

To define which host should be reachable through the second defined PDP context, a static route should be defined. As example, the site www.speedtest.net should be reachable via the second PDP context. The IP address of the site www.speedtest.net can be obtained by the ping as follows:

```
> ping www.speedtest.net
Pinging cs62.adn.xicdn.net [93.184.219.82] with 32 bytes of data:
Reply from 93.184.219.82: bytes=32 time=117ms TTL=51
Reply from 93.184.219.82: bytes=32 time=159ms TTL=51
```

In this case the IP address of the site www.speedtest.net is 93.184.219.82.

The following step depends on the operating system.

On Windows OS execute the following commands:

```
route ADD 93.184.219.82 MASK 255.255.255.255 37.177.17.130 METRIC 1 IF Ifnum
```

where Ifnum is the number of the RNDIS/CDC-ECM interface. This number can be recalled with the command:

```
route PRINT
```

On Linux OS execute the following commands:

```
route add -host www.speedtest.net gw 37.177.17.130
```

or

```
route add -net 93.184.219.82 netmask 255.255.255.255 gw 37.177.17.130
```

where usb0 is the name of the RNDIS/CDC-ECM interface provided with the command:

```
> ifconfig
```

As a proof of the validity of the configuration:

- Open a browser and go to the address www.speedtest.net
- In the bottom left angle of the page, the IP of the second defined PDP context will be reported because the traffic to the host www.speedtest.net is forwarded within the second PDP context.

- As countercheck, open a browser on a page displaying your IP address (like www.whatismyip.com): the displayed IP address corresponds to the IP associated to the first PDP context, which is used as default gateway that is “37.177.70.238”.

D Trace collection via RNDIS/CDC-ECM interface

TOBY-L2 series modules support the trace collection through the RNDIS/CDC-ECM interface. To record the trace log connect a socket to the module, hence the networking layer by means of the +UIPCONF AT command.

The configuration of the host networking layer shall be performed according with the TOBY-L2 module operating mode.

☞ For additional information about tracing capabilities, see TOBY-L2 / MPCI-L2 trace log application note [3].

D.1 Trace collection with TOBY-L2 in router mode

For the IPv4 configuration of TOBY-L2 module in router mode see section 3.2.1. The +UIPCONF AT command provides the IP configuration of the module (IP address and network mask).

The host RNDIS/CDC-ECM interface shall belong to the same TOBY-L2 subnetwork to start the IP communication.

If the host interface uses the automatic configuration (DHCP client), then the configuration shall be performed by the host IP stack, otherwise it needs to be performed manually.

Once the IP configuration is completed, use the IP address of the TOBY-L2 module to start the trace recording.

D.2 Trace collection with TOBY-L2 in bridge mode

For the IPv4 configuration of TOBY-L2 in bridge mode see section 2.2.1. The IP configuration of the RNDIS/CDC-ECM host interfaces shall be performed manually for every active context identifier, or automatically only for the preferred CID.

In bridge mode for each active PDP context/EPS bearer a virtual interface or interface alias shall be configured properly on the host. Furthermore, an additional virtual interface shall be configured to permit the communication between the TOBY-L2 IP stack and the IP stack of the host. The IP configuration of the TOBY-L2 IP stack can be retrieved via +UIPCONF AT command.

Once the IP configuration is completed, use the IP address of the TOBY-L2 module to start the trace recording.

D.3 Additional notes

To avoid any IP communication conflicts, all the subnetworks involved in the setup shall not interfere. The following subnetworks are involved: one for the RNDIS/CDC-ECM interface, one for every active PDP context/EPS bearer. In bridge mode every subnetworks has to be associated to its own virtual interface/interface alias.

E Advanced DNS configuration

This section provides further information regarding the DNS resolver implemented in the module. The provided information will cover the behavior of the URL resolution in these cases:

- single/multiple PDP contexts/EPS bearers and Wi-Fi STA connected to external hotspot
- single/multiple PDP contexts/EPS bearers and preferred DNS servers have been set (+UDNSCONF)
- single/multiple PDP contexts/EPS bearers and an IP address has to be ignored (+UDNSCONF)

From the point of view of the DNS servers, both active PDP context/EPS bearer and Wi-Fi external hotspot may provide up to 2 DNS servers each. The DNS replies of the used DNS servers are prone to different delays. Different delays may lead to unexpected behaviors, since the faster answer is taken into account by the resolver. Delays may occurs also due to recursive requests, as a DNS server may forward the DNS request to other DNS servers up to the root servers.

The following terminology will be adopted:

- Requester: this is the entity that requests the resolution of a specific URL
- DNS resolver: this entity is inside the module and has to provide the resolution of the URL requested by the requester
- Primary DNS_1: primary DNS of the oldest active context
- Secondary DNS_1: secondary DNS of the oldest active context
- Primary DNS_n: primary DNS of the latest active context
- Secondary DNS_n: secondary DNS of the latest active context
- Primary DNS_{STA}: primary DNS of the Wi-Fi interface in STA mode
- Secondary DNS_{STA}: secondary DNS of the Wi-Fi interface in STA mode
- DNS_{PREF1}: First preferred DNS server
- DNS_{PREFn}: Last preferred DNS server

Regarding the specific DNS server the following cases are possible:

- the DNS server is not reachable, hence the communication with it cannot be established;
- the DNS server is reachable, however the DNS response is delayed compared to other DNS responses;
- the DNS server is reachable and the DNS response contains a NXDOMAIN record; this means that the DNS server is not able to provide the public IP address that correspond to the requested URL;
- the DNS server is reachable and the DNS response contains an IP address: the IP address may correspond to the requested URL or in some cases it corresponds to a IP address of a HTTP/HTTPS server for advertisement purpose;
- The DNS server is reachable and the DNS response contains a REFUSED record, since there is an error in the request.

☞ For the DNS requests to be forwarded to the correct PDP context/EPS bearer, at every PDP context/EPS bearer activation a proper routing rule need to be added, otherwise all requests will be forwarded through the default gateway.

E.1 Single/multiple PDP contexts/EPS bearers and Wi-Fi STA connected to external hotspot

Figure 17 shows a simple example in which one PDP context/EPS bearer is active. Two DNS servers have been provided by the cellular network.

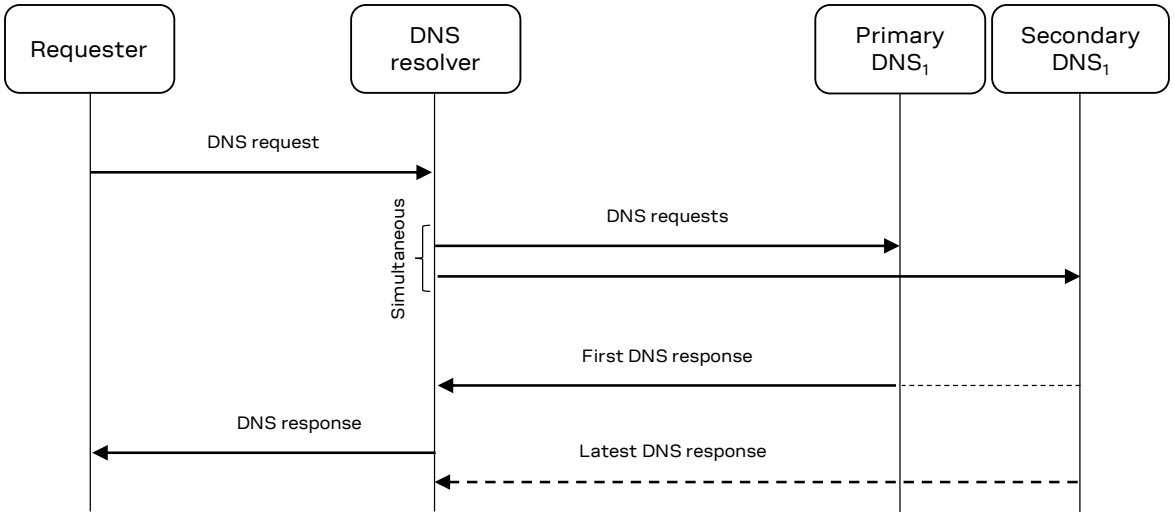


Figure 17: URL resolution when one PDP context/EPS bearer is active and two DNS servers provided by the cellular network

The DNS resolver simultaneously forwards the DNS request to DNS servers of the active context. The first DNS response is taken into account and forwarded back to the requester.

The example reported in Figure 18 consists of a larger list of DNS servers related to active PDP contexts/EPS bearers and Wi-Fi STA interface associated to the external hotspot.

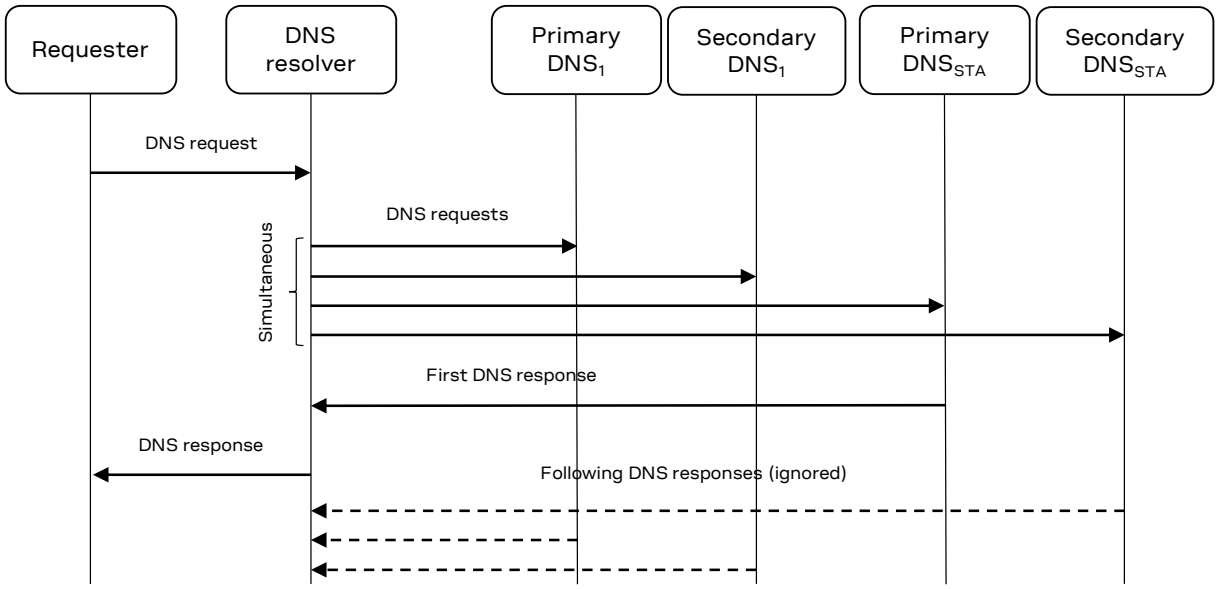


Figure 18: URL resolution when a list of DNS servers is related to active PDP contexts/EPS bearers and Wi-Fi STA interface associated to the external hotspot

The DNS resolver simultaneously forwards the DNS request to all available DNS servers. The list of available DNS servers consists of all the DNS servers provided by the cellular network at the PDP context/EPS bearer activation, and by the DNS server provided by the external Wi-Fi hotspot.

☞ The time of arrival of the DNS responses is driven by the network (cellular and Wi-Fi) latency, hence it is unpredictable.

E.2 Single/multiple PDP contexts/EPS bearers, preferred DNS server set (+UDNSCONF)

Figure 19 shows a complete flow of DNS requests/responses when there are several active PDP contexts/EPS bearers (DNS servers may be provided by the Wi-Fi external hotspot), and the user has defined additional DNS servers (preferred DNS servers) by means of the +UDNSCONF AT command.

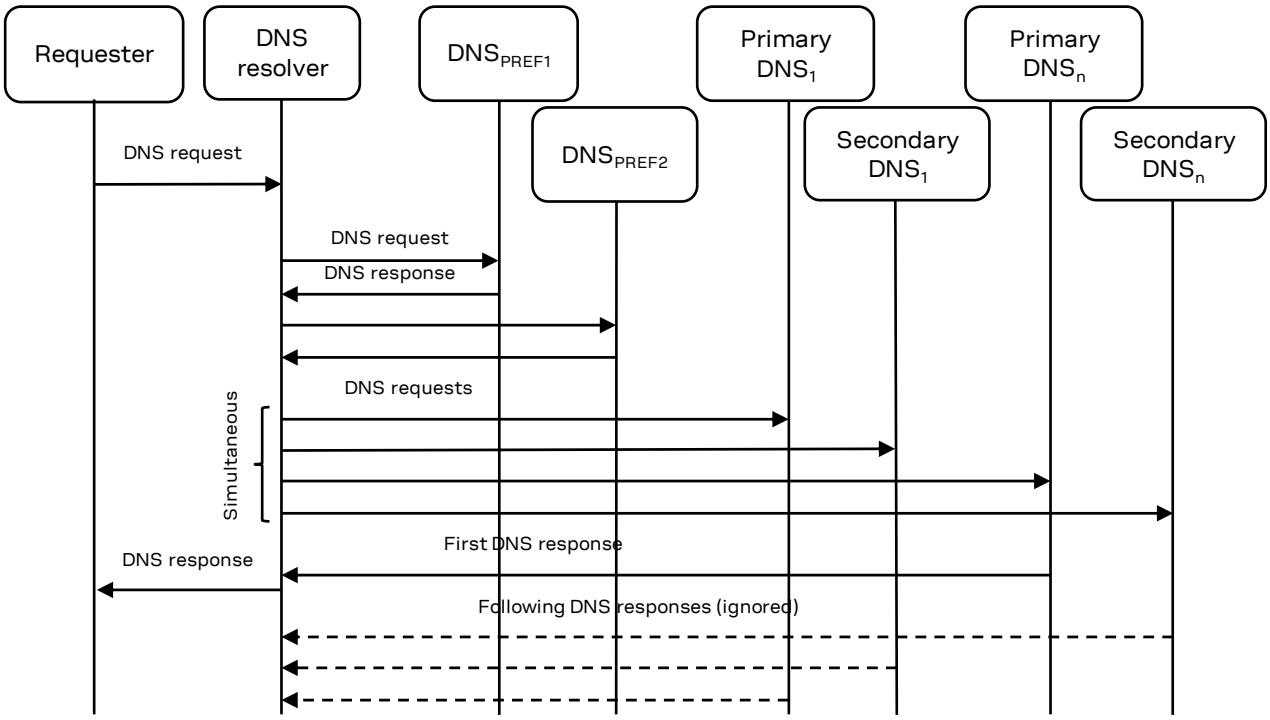


Figure 19: URL resolution in case of multiple PDP contexts/EPS bearers and additional DNS servers defined by the user

The DNS requests are first forwarded to preferred DNS servers. In the case that a successful reply (successful means: URL resolved, public IP address found) is received, the DNS resolver forwards the DNS response to the requester. Conversely, the list of preferred DNS servers is browsed one by one. Once the list has been exhausted the DNS request is broadcasted to the remaining DNS servers (not in the list of the preferred DNS servers). The first received reply is forwarded to the requester.

The preferred DNS feature can be used in the case, when the first DNS response contains a NXDOMAIN record, however further DNS responses contain the proper URL resolution. In this case the DNS server that replies with the proper IP may be added as the preferred DNS server.

E.3 Single/multiple PDP contexts/EPS bearers, IP address to be ignored set (+UDNSCONF)

Several DNS servers (mostly of them are the DNS servers of the network providers) instead of returning a NXDOMAIN record, return an IP address that does not correspond to the resolution of the requested URL. This IP address may corresponds to a HTTP/HTTPS server with advertisement purposes.

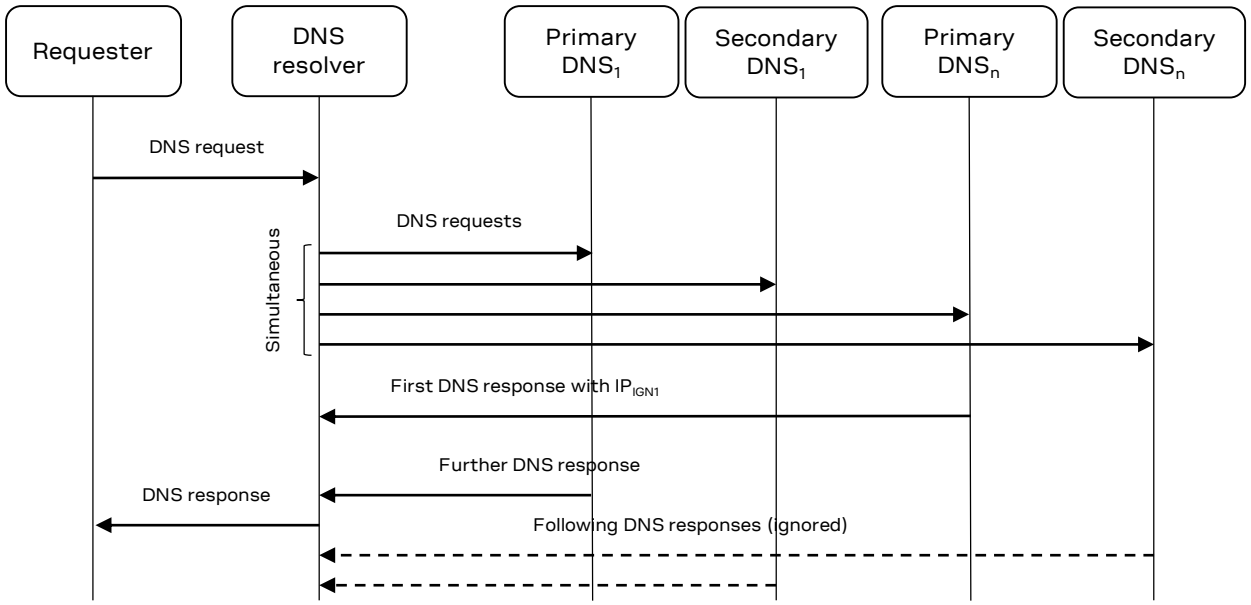


Figure 20: URL resolution in case of multiple PDP contexts/EPS bearers; first DNS response contains an IP address used for advertisement purposes

Figure 20 shows a complete flow of DNS requests/responses when the reply from primary DNS_n arrives for first. This replies contains an IP address IP_{IGN1} used for advertisement purposes. The reply seems correct (it has an IP address), however the obtained IP address does not correspond to the URL requested by the customer. By the use of the "ignore IP address" feature, the IP address of the advertisement server can be ignored, since it is considered as a NXDOMAIN reply. Consecutively, the received DNS response will be ignored in favor of further received DNS responses (in the example a further DNS response is arriving from primary DNS_1).

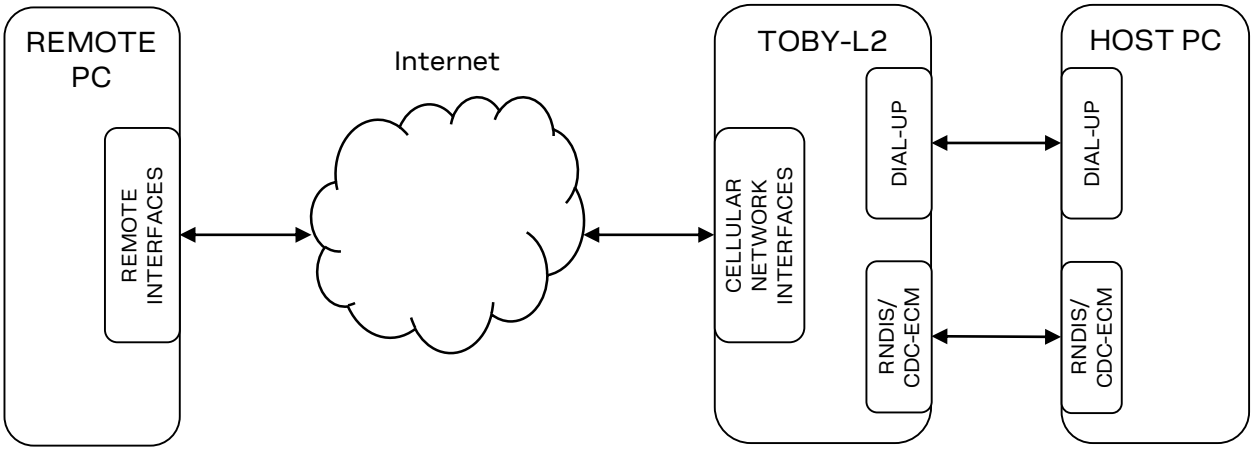
E.4 Additional methods for DNS request/response filtering (+UIPTABLES/+UIP6TABLES)

The DNS requests/responses can be filtered by the use of the module firewall. The filtering can be performed on the INPUT/OUTPUT chain by the use of the +UIPTABLES AT command for the IPv4 traffic and by the use of the +UIP6TABLES AT command for the IPv6 traffic. The filtering of the DNS request on the INPUT chain will prevent the resolver to reach the DNS server, while the filtering on the OUTPUT chain will lead the resolver to wait the expiration of the request timeout. The filtering can be performed on the bases of the destination/source address, destination/source port, and on the string (characters or hexadecimal values) that are contained in the packet.

F MTU characterization

This section provides additional information regarding the maximum transmission unit (MTU). The concept of maximum transmission unit can be applied to several layers of communication protocols, however the MTU properly denotes the maximum length of an IP packet. In the case of the TCP/IP communication, the IP packet consists of the IP header (typically 20 bytes) and of the IP Packet Data Unit (PDU). The IP packet PDU consists of the TCP header (typically 20 bytes) and of the TCP packet data unit. The length of the TCP packet data unit is named Maximum Segment Size (MSS). For a TCP/IP packet sent over Ethernet computer networking technology the MTU size is 1500 bytes. Considering the IP and the TCP header the corresponding MSS has 1460 bytes (MSS = MTU - IP header - TCP header). The value is present in [SYN] and [SYN, ACK] packets, when the TCP/IP connection is going to be established.

The MTU value is associated with the communication interface, and can differ from interface to interface. In TOBY-L2 series modules there are several communication interfaces to be considered. The following diagram shows the interfaces, where MTU values need to be taken into account to estimate the MTU used for the data transfer:



- MTU of the REMOTE INTERFACE on the REMOTE PC: this value is unknown, since it has to be discovered during the communication establishment. A typical value for an Ethernet interface is 1500 bytes. Furthermore, in the Verizon cellular network the default MTU is 1428 bytes, while in the AT&T cellular network the default MTU is 1430 bytes.
- MTU of the CELLULAR NETWORK INTERFACE on TOBY-L2 module: this value is obtained from the cellular network and it is contained in the Protocol Configuration Options (PCOs). The default value is 1500 bytes. Furthermore, in the Verizon cellular network the default MTU to be used is 1428 bytes, while in the AT&T cellular network the default is 1430 bytes.
  -
- MTU of the DIAL UP on HOST PC: this value is typically set to 1500 bytes as on Ethernet interfaces.
- MTU of the RNDIS/CDC-ECM on HOST PC: this value is typically set to 1500 bytes as on Ethernet interfaces.

The use of the correct MTU value will avoid IP fragmentation and the most effective data transfer will be achieved. The concept of the MTU is valid for the TCP/IP connection, while UDP/IP connection does not implement it. At the TCP/IP connection establishment the source peer sets the MSS value in the [SYN] packet on the bases of the interface MTU. The destination peer receives the [SYN] packet with the source peer MSS, and replies with a [SYN, ACK] packet specifying its own MSS. Once the source peer receives the [SYN, ACK] packet selects the minimum MSS size and use it in the TCP/IP connection. However, along the way between the source and destination peers may exist some network segments with lower MTU. In that cases, the IP packets are fragmented in more packets increasing the overhead of the communication. The packets are then reassembled. The IP protocol

implements the “Path MTU discovery”, which will be used to define the lowest MTU along the path in order to avoid fragmentation. However, the MTU discovery mechanism may not work due to security restrictions adopted on several networks (e.g. ICMP packet dropping to prevent denial-of-service attack).

MTU settings on UE side are automatic and already satisfied according to each MNO requirements when module’s own Internet protocol transport layer is used for user data connectivity.

The RNDIS/CDC-ECM and PPP do not negotiate the MTU size, hence the suggestion is to verify and properly set the MTU on the HOST PC for the following cases:

- Verizon cellular network provider set the MTU of the dial-up and RNDIS/CDC-ECM interfaces to 1428 bytes;
- AT&T cellular provider set the MTU of the dial-up and RNDIS/CDC-ECM interfaces to 1430 bytes;

In all the cases not included in the previous list, the MTU for the dial-up and RNDIS/CDC-ECM interfaces is set to 1500 bytes. If needed, the adopted MTU should be verified and set accordingly.

G Dial-up with TOBY-L210-62S

The section provides an example on how to manage dial-up connections when the initial default EPS bearer and IMS context are active. The examples are operating system independent.

G.1 Prerequisites

The TOBY-L210-62S must operate in a “Fairly backwards-compatible” configuration (AT+UUSBCONF=0), since it allows a PPP dial-up connection to start on an already active PDP context/EPS bearer. For more details, see section 4.2.

Configure the initial default bearer with the required internet PDN (APN and authentication algorithm) by means of AT+UCGDFLT command.

During the LTE registration the initial default bearer is automatically activated on CID=4. If the IMS service is available, then the DUT will activate the IMS default bearer on CID=8.

Command	Response	Description
AT+UUSBCONF?	+UUSBCONF: 0,"",,"0x1141" OK	Check that module is in 'Fairly back-compatible' configuration, if not, set this mode (see the u-blox AT commands manual [1]).
AT+CFUN=4	OK	Set the module in airplane mode.
AT+UCGDFLT=1,"IP","<apn>",,,,,,,,,,,,,,,,,,,,,1,"<user>","<pass>"	OK	Configure the initial default EPS bearer for LTE network to ensure connectivity on it.
AT+CFUN=1	OK	Sets the MT to full functionality.

G.2 Scenarios

To use dial-up there are two alternative cases.

G.2.1 Dial-up over the initial default EPS bearer

The dial-up connection will provide connectivity over the initial default EPS bearer. The CID =4 and the CID=8 are both active.

Command	Response	Description
ATD*99***4#		Perform the dial-up on the initial default EPS bearer.

Once the dial-up connection is terminated the EPS bearer at CID=4 is disconnected and it is locally undefined. The connectivity is no more available at CID=4. Hence, further dial-up connections will be performed on another CID, which will be defined.

Command	Response	Description
AT+CGDCONT=1,"IP","<apn>"	OK	Define the default EPS bearer on CID=1.
AT+UAUTHREQ=1,1,"<user>","<pass>"	OK	Configure the authentication parameters for the initial default EPS bearer for LTE network.
ATD*99***1#		Perform the dial-up on the default EPS bearer on CID=1.

Once the new CID (not on initial default EPS bearer) is defined, after the dial-up disconnection the CID will remain locally defined. Further dial-ups do not need redefinition of the CID.

G.2.2 Local dial-up

The local dial-up establishes a PPP communication between the DTE and the module through a serial interface (UART, MUX, or CDC-ACM). For more details see section 4.3.

Local dial-up feature will not perform PDN deactivation, thus preventing the initial default EPS bearer to become locally undefined as in the previous case.

Command	Response	Description
`ATD*99***100#`		Perform the local dial-up.

H Mobile terminated EPS bearer/PDP context enumeration rules

The CID of a mobile terminated EPS bearer/PDP context is assigned according to the rules below:

- Primary PDP context (2G/3G) or default EPS bearer (4G): first CID not defined in the ordered list = [4, 3, 2, 1, 8, 7, 6, 5]
- Secondary PDP context (2G/3G) or dedicated EPS bearer (4G): first CID not defined in the ordered list = [8, 7, 6, 5, 1, 2, 3, 4]

Example:

An example of the enumeration rule occurring in 4G networks is presented in the following:

Command	Response	Description
AT+CGDCONT?	+CGDCONT: 4,"IP","ims.mnc010.mcc222.gprs","93.68.170.89",0,0,0,0,0 OK	Check if there is connectivity on the initial default bearer (4G network).
AT+CFUN=4	OK	Set the module in airplane mode to configure the default PDP context for LTE network.
AT+UCGDFLT=1,"IP",web.omnitel.it"	OK	Configure the initial PDP context for LTE network.
AT+CFUN=1	OK	Sets the MT to full functionality.
AT+CGDCONT?	+CGDCONT: 4,"IP","web.omnitel.it.mnc010.mcc222.gprs","37.177.70.238",0,0,0,0,0,0 OK	In this case the initial default EPS bearer is on CID 4.

Command	Response	Description
AT+CFUN=4	OK	Set the module in airplane mode.
AT+CGDCONT=4,"IP","wap.tim.it"	OK	Configure the EPS bearer on CID 4 for LTE network.
AT+UCGDFLT=1,"IP","ibox.tim.it"	OK	Configure the initial EPS bearer for LTE network.
AT+CFUN=1	OK	Set the MT to full functionality.
AT+CGDCONT?	+CGDCONT: 3,"IP","ibox.tim.it.mnc001.mcc222.gprs","10.161.25.60",0,0,0,0,0,0 +CGDCONT: 4,"IP","wap.tim.it","",0,0,0,0,0,0 OK	In this case the initial default EPS bearer is on CID 3, since the CID 4 was already defined.

I RNDIS optimization and Linux kernels

☞ The section is applicable to Linux kernel version greater than 4.8.

☞ The section is applicable to TOBY-L2 / MPCI-L2 "00S", “01S”, “02S”, “60S” and “62S” product versions and to TOBY-L200-03S-00, TOBY-L210-03A-00, TOBY-L210-03S-00, TOBY-L280-03S-00.

The RNDIS interface may not work if Linux kernel version of the DTE is higher than 4.8 and RNDIS driver optimization is enabled (AT+UDCONF=67,1). The reported behavior is due to the “rndis_host: Set valid random MAC on buggy devices” patch introduced in the Kernel version v4.8-rc1:

https://github.com/torvalds/linux/commit/a5a18bdf7453d505783e40e47ebb84bfdd35f93b#diff-6dfe16ca0bdcdc21501ef11cfd202a10

The patch presents an incompatibility with the RNDIS driver optimization, which leads to a TCP and UDP traffic lost.

The issue is not present if the RNDIS driver optimization is disabled (AT+UDCONF=67,0), however this may lead to lower throughput.

J Uplink filter disable and source base routing in bridge mode

J.1 State of art

TOBY-L2 series modules support two operating modes: router and bridge mode. For the scope of this topic only the bridge mode is relevant. In bridge mode the IP termination is on the host, since the target IP stack is not involved in the networking. At every PDP context/EPS bearer activation the networking configuration needs to be set on the host RNDIS/CDC-ECM interface. The IP address of the PDP context/EPS bearer (provided by +CGDCONT AT command) shall be configured on the host RNDIS/CDC-ECM, while the IP address provided by +UIPADDR AT command shall be use as gateway (default gateway or gateway for a specific IP address or IP range).

The uplink/downlink data path consists of following elements: RNDIS/CDC-ECM driver, cellular interface (CCINET) driver. In the uplink the packets arriving from the host RNDIS/CDC-ECM are received by the target RNDIS/CDC-ECM. Once they are received, they are forwarded to the CCINET driver. The CCINET driver on the bases of the source IP address is able to define on which PDP context/EPS bearer the packet should be transmitted. The source IP address of the packet is compared with the IP addresses of every active PDP context/EPS bearer. If no IP address match is found then the packet is discarded. For the downlink the packets are received at the CCINET driver and forwarded to the RNDIS/CDC-ECM driver. The packets are then transmitted to the host, and the host RNDIS/CDC-ECM driver will acquire the packets and forward them to the host IP stack.

In case of multiple PDP contexts/EPS bearers several IP aliases (virtual interfaces for Linux OS) should be configured with proper IP addresses.

J.2 Bridge mode with disabled uplink filter

As described in the appendix J.1, TOBY-L2 is not completely transparent in terms of IP communications, since the packets are discarded when no match is found between the source IP address and the IP addresses of the active PDP contexts/EPS bearers. However this "uplink filter" can be disabled with the +UDCONF=9,2 AT command. In this case the packets with no matching are transmitted on the first active context (considering the active PDP context/EPS bearer from CID 1 to 8). Disabling the uplink filter implies also that in the case of multiple PDP contexts/EPS bearer all the packets are transmitted on the first active context.

J.3 Test scenario

J.3.1 Requirement

- Linux OS PC: RNDIS, Ethernet interface
- TOBY-L2 series module

J.3.2 Scenario: bridge mode with disabled uplink filter

The host PC is connected to TOBY-L2 via the RNDIS interface. On the host PC a bridge is created to merge the Ethernet and the RNDIS interface. Only one PDP context/EPS bearer is active, and the RNDIS interface of the HOST is properly configured. On the Ethernet side of the host PC there is a subnetwork, whose packets are forwarded by the PC via the bridge to the RNDIS interface. The TOBY-L2 transmits the packets of the subnetwork on the active PDP context/EPS bearer. In this case, the cellular network provider will route the packets to a specific private subnetwork. The downlink packets from the private subnetwork are received by TOBY-L2 and it will forward them to the RNDIS interface. The host PC will forward the packets through the bridge to the Ethernet interface.

K Optimal throughput on a Linux system

☞ The section is applicable to TOBY-L201 / MPCI-L201 and TOBY-L2 / MPCI-L2 "00S" and “60S” product versions.

On a Linux system, to reach the maximum throughput it is necessary to recompile the kernel. Apply the following modification in `/kernel/drivers/net/usb/usbnet.c`:

Replace "`size_t size = dev->rx_urb_size; `" with "`size_t size = (16*1024);`"

If it is not possible to recompile the kernel, then try to use CDC-ECM.

As last resort try to use the following command:

```
AT+UDCONF=67,0
```

This command disables the RNDIS driver optimization and could mitigate the effects in router mode only.

L List of acronyms

Abbreviation	Definition
ACM	Abstract Control Model
APN	Access Point Name
ARP	Address Resolution Protocol
AT	AT Command Interpreter Software Subsystem, or attention
UART	Universal Asynchronous Receiver-Transmitter serial interface
CDC	Communications Device Class
CID	Context Identifier
CM	Connection Manager
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DTE	Data Terminal Equipment
ECM	Ethernet networking Control Model
EPS	Evolved Packet System
GPS	Global Positioning System
GSM	Global System for Mobile Communication
ICMP	Internet Control Message Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LCP	Link Control Protocol
LTE	Long Term Evolution
MAC	Media Access Control
MT	Mobile Terminated
MTU	Maximum Transmission Unit
NA	Neighbor Advertisement
NAT	Network Address Translation
NDP	Neighbor Discovery Protocol
NS	Neighbor Solicitation
NVM	Non Volatile Memory
OS	Operating System
PDP	Packet Data Protocol
PDN	Packet Data Network
PPP	Point-to-Point Protocol
PS	Packet Switched
RA	Router Advertisement
RAT	Radio Access Technology
RS	Router Solicitation
RNDIS	Remote Network Driver Interface Specification
SAP	SIM Access Profile
TCP	Transfer Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System

Abbreviation	Definition
URC	Unsolicited Result Code
URL	Uniform Resource Locator
USB	Universal Serial Bus

Table 2: Explanation of the abbreviations and terms used

Related documents

[1] u-blox AT commands manual, UBX-13002752
[2] u-blox AT commands examples application note, UBX-13001820
[3] u-blox TOBY-L2 and MPCI-L2 trace log application note, UBX-14042262
[4] Charles M. Kozierok – "The TCP/IP Guide" – No Starch Press
[5] Andrew S. Tanenbaum – "Computer Networks (5th Edition)" – Prentice Hall
[6] RFC 2131, Dynamic Host Configuration Protocol, https://www.ietf.org/rfc/rfc2131.txt
[7] RFC 1661 The Point-to-Point Protocol (PPP), ftp://ftp.rfc-editor.org/in-notes/rfc1661.txt
[8] RFC 4861 Neighbor Discovery for IP version 6 (IPv6), ftp://ftp.rfc-editor.org/in-notes/rfc4861.txt
[9] RFC 4862 IPv6 Stateless Address Autoconfiguration, ftp://ftp.rfc-editor.org/in-notes/rfc4862.txt
[10] RFC 5072, IP Version 6 over PPP, ftp://ftp.rfc-editor.org/in-notes/rfc5072.txt
[11] RFC 5075 IPv6 Router Advertisement Flags Option, ftp://ftp.rfc-editor.org/in-notes/rfc5075.txt
[12] RFC 6106 IPv6 Router Advertisement Options for DNS Configuration ftp://ftp.rfc-editor.org/in-notes/rfc6106.txt
[13] RFC 6459 IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS), ftp://ftp.rfc-editor.org/in-notes/rfc6459.txt
[14] RFC 793 Transmission Control Protocol – Protocol Specification – Darpa Internet Program Protocol Specification, ftp://ftp.rfc-editor.org/in-notes/rfc793.txt

☞ For regular updates to u-blox documentation and to receive product change notifications, register on our homepage (www.u-blox.com).

Revision history

Revision	Date	Name	Comments
R01	29-Oct-2014	ador	Initial release
R02	30-Jan-2015	mace	Added some suggestion on Connection Manager development and kernel recompiling
R03	17-Jul-2015	mace	Added local PPP description
R04	19-Oct-2017	lpah	Multiple PDP contexts in router/bridge mode and dial-up description added
R05	10-Jun-2020	ador	Added DHCP in bridge mode, DNS handling for multiple context scenario, RNDIS not working for kernel greater than 4.8

Contact

For complete contact information, visit us at www.u-blox.com.

u-blox Offices

North, Central and South America

u-blox America, Inc.

Phone: +1 703 483 3180
E-mail: info_us@u-blox.com

Regional Office West Coast:

Phone: +1 408 573 3640
E-mail: info_us@u-blox.com

Technical Support:

Phone: +1 703 483 3185
E-mail: support@u-blox.com

Headquarters
Europe, Middle East, Africa

u-blox AG

Phone: +41 44 722 74 44
E-mail: info@u-blox.com
Support: support@u-blox.com

Asia, Australia, Pacific

u-blox Singapore Pte. Ltd.

Phone: +65 6734 3811
E-mail: info_ap@u-blox.com
Support: support_ap@u-blox.com

Regional Office Australia:

Phone: +61 2 8448 2016
E-mail: info_anz@u-blox.com
Support: support_ap@u-blox.com

Regional Office China (Beijing):

Phone: +86 10 68 133 545
E-mail: info_cn@u-blox.com
Support: support_cn@u-blox.com

Regional Office China (Chongqing):

Phone: +86 23 6815 1588
E-mail: info_cn@u-blox.com
Support: support_cn@u-blox.com

Regional Office China (Shanghai):

Phone: +86 21 6090 4832
E-mail: info_cn@u-blox.com
Support: support_cn@u-blox.com

Regional Office China (Shenzhen):

Phone: +86 755 8627 1083
E-mail: info_cn@u-blox.com
Support: support_cn@u-blox.com

Regional Office India:

Phone: +91 80 405 092 00
E-mail: info_in@u-blox.com
Support: support_in@u-blox.com

Regional Office Japan (Osaka):

Phone: +81 6 6941 3660
E-mail: info_jp@u-blox.com
Support: support_jp@u-blox.com

Regional Office Japan (Tokyo):

Phone: +81 3 5775 3850
E-mail: info_jp@u-blox.com
Support: support_jp@u-blox.com

Regional Office Korea:

Phone: +82 2 542 0861
E-mail: info_kr@u-blox.com
Support: support_kr@u-blox.com

Regional Office Taiwan:

Phone: +886 2 2657 1090
E-mail: info_tw@u-blox.com
Support: support_tw@u-blox.com