aculab

ACULAB.COM

Prosody X

Network Integration guide

MAN1763

PROPRIETARY INFORMATION

Document Revision

Rev	Date	By	Detail
6.4	17-01-07	djl	Initial release for V6.4 telephony software support
6.5	14-01-13	mb	Amendment for V6.4 telephony software support
6.5.1	22-01-13	ebj	Reformatted and updated to corporate fonts.
6.6.0	27-04-15	pgd	Align with 6.6 distribution
6.7.0	11-04-17	pgd	Add DHCP advice
6.7.1	06-09-18	pgd	Clarify port numbers for 1U enterprise
6.8.0	2-11-22	pgd	Rework and align with 6.8 release, move flash to another doc, simplify security section
6.8.1	10-11-22	pgd	Reformat

CONTENTS

1 Introduction

The 6.8 Aculab telephony software distribution supports following network attached TDM signalling and media processing chassis:

- Prosody X Evo chassis
- Prosody X HA chassis
- Prosody X 1U enterprise chassis

These chassis present Prosody X TDM signalling and media processing resources over an IP network to applications using Aculab APIs, and are managed by Aculab telephony software installed and running on a Linux or Windows controlling host.

This document provides information on how Prosody X chassis are integrated into the IP network environment. All chassis types support IPv4. Only the Evo and HA chassis types support IPv6.

Prosody X TDM and media processing resources are presented over the network as Prosody X cards – the Prosody X HA chassis may be fitted with one or two Prosody X cards, the other types of chassis present a single Prosody X card to the controlling host. In the case of the Prosody X Evo, the physical PPC/DSP based Prosody X card of older chassis types are replaced by processes running on the chassis CPU but from controlling host point of view, the TDM and media processing resources are still managed and presented as a Prosody X card, and are referred to as such in this document.

Prosody X cards are configured using ACT (Aculab configuration tool) or `prosody_ip_card_mgr`, a command line tool providing the same functionality.

This document is applicable to distributions 6.8 and later of the Aculab V6 Telephony software.

2 How chassis are brought into service

2.1 Card boot

A Prosody X card in a TDM signalling and media processing chassis boots from local flash memory into a basic state capable of interacting with a controlling host over the IP network. To become fully operational the card needs to complete its boot process by interacting with a controlling host and downloading further software from that host. In order to begin this process, the card broadcasts low-level protocol 'boot me' packets which request a controlling host to boot it fully.

A low level protocol is used because, at boot time, the card has no assigned IP address. One consequence of using such a low level protocol is that only hosts on the same switched network as the card can boot it - low level protocol packets do not pass through routers. The low level protocol packets have an “eth.type” of 0x08ff.

A controlling host will reply to a 'boot me' packet if the card is in its list of Prosody X cards that it has been configured to boot. A 'boot me' packet contains the serial number of the presented Prosody X card, MAC address information and various sub-fit details such as the numbers of telephony ports and media processing modules.

When a host replies to a 'boot me' packet, it sends a low-level protocol packet containing sufficient information for the card to obtain an IP set-up. If more than one host replies, the one whose reply is received first will boot the card. Once the card has obtained an IP address, it sends this to the host using the low level protocol and the remainder of the boot sequence is achieved over TCP. This consists of downloading various files from V6 telephony software installation on the controlling host to the card/chassis and starting various processes on it. The stages occurring during the boot process will be displayed in the Diagnostics/Status columns on the ACT "Prosody X settings" page or in output of `prosody_ip_card_mgr` “list“ subcommand. Once the boot sequence has completed, the card is usable and will appear in the ACT main card list and will be shown as having the state "In Service" in the list displayed on the ACT "Prosody X settings" page or in output of `prosody_ip_card_mgr` “list“ subcommand.

2.2 Additional hosts

In the case where an additional host is required in order to allow applications on that host to use card (booted by controlling host), it is necessary for that additional host to have a procedure to discover the card.

The way in which this discovery is initiated depends on how the card appears in the additional host's Prosody X card list. If the card is specified with a static IP address, the host initiates contact with it using TCP. Otherwise, the host does not know the address of the card and must therefore initiate contact with it using the low level protocol. As in the case for booting host, use of low level protocol will work only when the card is on the same switched network as the additional host.

WARNING

If cards have additional hosts, care must be taken that only one host is configured to download and configure signalling and (for non Evo chassis types) TiNG firmware.

2.3 Host maintained card lists

Controlling (and additional) hosts maintain a Prosody X card list of all chassis presented Prosody X cards that the host would like to appear as "In Service" along with information to allow the host to boot or discover each one. In ACT this list is shown on ACT "Prosody X settings" page.

Cards must be added to the Prosody X card list manually. This may be achieved either by using the ACT or `prosody_ip_card_mgr` command line tool or the Aculab Resource API `acu_register_prosody_ip_card()` function. Similarly, they may be removed either by using the ACT or `prosody_ip_card_mgr` or the Aculab Resource API `acu_unregister_prosody_ip_card()` function.

Each entry in the Prosody X Settings list specifies:

- If the host can boot the card and, if so, what IP set-up it should give it;
- If the card watchdog should be enabled and with what timeout.

This information is provided either when the card is added to the list (see above) or by using the ACT or the Aculab Resource API `acu_configure_prosody_ip_card()` function to modify an existing entry.

Specifying that a host can boot a card means that the host will try to boot the card if it receives a low level 'boot me' packet from it. It does not mean that the host will always boot the card – just that it will attempt to do so if the opportunity arises. Specifically, if a card is already booted then the parameters provided are used only to discover the card (see the 'Additional hosts' section above) and are not imposed on it.

A Prosody X card contains a watchdog which may be configured as part of the boot process. If enabled, this will restart the card if any of the following occurs for longer than the specified timeout period:

- Certain card processes failing to 'kick' the watchdog
- Absence of host maintaining a TCP connection with the card (i.e. no host having the card in its main card list)

The watchdog may be useful in cases where physical access to chassis presenting card is difficult. However, unless such operational considerations oblige, it is normally better not to enable the watchdog so that, in the event of a card failure of some kind, the card state will not be lost on a watchdog restart, and thus it will be possible to retrieve diagnostic data in collaboration with advice from Aculab support.

2.4 Card failure to come into service

This section covers a number of problems that may occur when booting and discovering cards, and suggests ways of fixing them.

Check the host's routing table to confirm that outgoing IP packets sent to the card's IP address (or, if it's not yet booted, the address you intend to boot it with) can actually get to the card. If there is no route for such packets to reach the card, change the routing table so that there is. If there is more than one route then check that each of them is valid. If all such routes are not valid, then communications with the card may be intermittent or non functional.

Has another host booted the card? If so, and the card has been entered in the Prosody X card list with a static IP address, your host will not be able to successfully discover the card without this address matching the current address of the card. The list entry can be viewed, for example, by using the ACT.

If the card can only be accessed from your host via a router (i.e. is on a different switched network) then, because of low level protocol used for booting, your host cannot boot the card and another host must do so. The card must be entered in the Prosody X card list of the additional host with a static IP.

3 IP Network environment

3.1 Network requirements

Prosody X chassis must be connected to a switched and/or routed low packet latency full duplex network.

Prosody X Evo and Prosody X HA chassis support Ethernet link speeds of up to 1000Mbs full duplex, whereas Prosody X 1U chassis only supports link speeds of up to 100Mbs full duplex, use of a network supporting use of at least these rates is recommended.

Use of Ethernet hubs in any part of this network, which carries Prosody X media or control traffic must be avoided. If routers are used, they must be able to sustain the bandwidth required.

Prosody X uses Ethernet bandwidth for control (e.g. call, switch or TiNG APIs) and RTP (used to carry VoIP media) for IP telephony. Of these, the TiNG API and RTP will generally be the dominant users.

As the bandwidth limit of an Ethernet is approached, performance degrades in two main ways:

- The proportion of packets lost increases.
- The delays in packet transmission become less predictable. This variability is termed jitter.

The effects of increases in these figures depend on the high level protocols in use:

- IP Telephony: RTP is used to transmit media, generally audio. The receiver's Jitter Buffer will trade delay with the proportion of packets arriving too late to be inserted into the decoded media stream in an attempt to maximise perceived audio quality in terms of both delay and fidelity. Increases in the delay and jitter lead to a reduction in received quality, dependant on the codec type and performance of receiver's Packet Loss Concealment (PLC) algorithm.
- Call and Switch APIs: TCP is used here and, as it's a reliable protocol, increases in the above figures lead to a higher proportion of retransmissions, resulting in more bandwidth being used and slower response times.
- TiNG API: The protocol used here is also reliable, so increases in the above figures lead to higher proportion of retransmissions, resulting in more bandwidth being used and slower response times which may lead to underruns/overruns for play/record type activities

Prosody X must be used on networks where little or no TCP packet fragmentation occurs and UDP fragmentation does not occur in path between controlling/additional host and card.

3.2 IP address requirements

The number of IP addresses required by a Prosody X card depends on chassis type and whether IPv4 or IPv6 addresses are being used.

- Prosody X 1U enterprise chassis only supports a single IPv4 address.
- Prosody X HA chassis support both IPv4 and IPv6, for IPv4 each Prosody X card presented by chassis has its own IPv4 address, whereas for IPv6 additional IPv6 addresses are required for each Prosody X card DSP.
- Prosody X Evo chassis support both IPv4 and IPv6 addresses, and for each

IP type either a single address card be used for the presented Prosody X card, or an additional address can be assigned for (RTP) media use (the additional address is associated with second media specific RJ45 ethernet connector.

IP addresses maybe assigned static IP addresses, addresses assigned by DHCP, or for IPv6, addresses assigned through IPv6 SLAAC. Typically for production systems the use of statically assigned IP addresses is recommended.

Use of temporary IPv6 addresses is not recommended as their expiration may lead to addressing problems.

4 Security considerations

4.1 Network security assumptions

It is assumed the local switched network is itself secure and that any host that bootstraps and / or controls a Prosody X card is itself secure. Traffic between the controlling host and Prosody X card is not encrypted.

4.2 Configuring firewalls

Here is a list of Prosody X PCI TCP and UDP ports which should be blocked against traffic originating from anywhere other than the controlling host machine. Note that the ports may change with future card revisions.

Protocol	Port
TCP	220 (ppcctld), 222 (hdirelay), 2031 (asspmon), 3013 (TDM switch), 6614 (STUN), 8190 (IPTel), 8191 (TRM), 6583 (alive/utility)
UDP	2030 (cardinfod)
UDP	*Evo chassis* 16384 — 16386 (debug, ASSP, ASSP mon) *HA chassis:* 16384 — 16386, 24576 — 24578, 32768 — 32770, 40960 — 40962 (DSP 0 — 3 debug, ASSP, ASSPmon) *1U enterprise chassis:* 16384 — 16386, 40960 — 40962 (DSP 0 — 1 debug, ASSP, ASSPmon)

Alternatively, all Prosody X TCP and UDP ports apart from those in the list below should be blocked against traffic originating from anywhere other than the controlling host machine.

Protocol	Port
UDP	*Evo chassis* 50000-65531 (RTP, RTCP et al) *HA chassis:* 16387 — 17407, 24579 — 25599, 32771 — 33791, 40963 — 41983 (DSP 0 — 3 RTP, RTCP et al) *1U enterprise chassis:* 16387 — 17407, 40963 — 41983 (DSP 0 — 1 RTP, RTCP et al)

4.3 Card security key

When a card is added to Prosody X card list on controlling or additional host, a card security key is specified.

Only applications with knowledge of the security key can interact with Prosody X card resources.

The security key is stored in plain text on the host file system, and is also visible on local network during chassis boot (but only in a unicast packet sent from host to chassis).

NOTE

Any host on the local network has the ability to restart a Prosody X chassis without requiring knowledge of card security key through transmission of a low level protocol restart packet.

It is thus important that the local switched network is secure and that low-level protocol packets (of eth.type 0x08ff) can only originate from this network.

Contact us

Phone

+44 (0)1908 273800 (UK)
+1(781) 352 3550 (USA)

Email

Info@aculab.com

Sales@aculab.com

Support@aculab.com

Socials

Certificate number IS 722024
ISO 27001:2013

Certificate number FS722030
ISO 9001:2015