Tele2 Växel
Trio Connect
Network deployment information

TELE2
FÖRETAG

About this document

This document describes hosts and ports for various types of traffic to and from Tele2s network for Tele2 Växel and Trio Connect.

The document will be updated upon changes in the service platform and/or surrounding systems.

We recommend that you occasionally revisit the document to ensure that your firewall has the correct settings at all times.

For whom is this document?

This instruction is aimed at personnel with sufficient knowledge in configuring the company firewall.

Update April 2020

A new firmware server for Mitel desk phones was added, as the previous server has been removed.

New host:
193.12.60.49 (firmware.tele2vaxel.se) port 80

Update September 2018

During fall 2018, the platform was expanded with additional edge nodes, for which new networks have been added in this document wherever communication with the platform is described.

The complete set of networks are:
213.100.32.64/27
213.100.32.240/28 (New)
213.100.33.0/28 (New)

Contents

1 Customer Firewall/CPE settings

Host	Direction	Destination port	Protocol	Transport	Comments
Tele2 tele2vaxel.se 213.100.32.64/27 213.100.32.240/28 213.100.33.0/28	Outgoing	443	HTTP(S)	TLS	Web services, e.g. downloading software using secure HTTP, Microsoft Exchange calendar integration
Tele2 tele2vaxel.se 213.100.32.64/27 213.100.32.240/28 213.100.33.0/28	Incoming* Outgoing	5061	SIP(S)	TLS	Signalling between Tele2 and connected devices. SIP inspection must in some cases be disabled in the firewall
Tele2 tele2vaxel.se 213.100.32.64/27 213.100.32.240/28 213.100.33.0/28	Incoming* Outgoing	49152 - 65535	(S)RTP/RTCP	UDP	Media/speech traffic for Mitel 6800 devices, Tele2's Softphone and other IP devices. Ports within this range are randomly allocated when the call is set up.
Tele2 tele2vaxel.se 213.100.32.64/27 213.100.32.240/28 213.100.33.0/28	Outgoing	123	NTP	UDP	Time synchronization between Tele2 and connected devices
1.1 Mitel devices					
Mitel rcs.aastra.com**	Outgoing	80/443	HTTP(S)	TCP	Mitel device settings distribution via the supplier's redirection system
Mitel 1.aastra.pool.ntp.org** 2.aastra.pool.ntp.org** 3.aastra.pool.ntp.org**	Outgoing	123	NTP	UDP	Time synchronization during the auto-configuration process for Mitel 6800 devices
Tele2 firmware.tele2vaxel.se 193.12.60.49	Outgoing	80	HTTP	TCP	Firmware repository for Mitel 6800 devices
1.2 Mediatrix 4102S, C710, C711 and S7 series					
Tele2 213.100.32.64/27 213.100.32.240/28 213.100.33.0/28	Incoming* Outgoing	5004 – 5134	(S)RTP/RTCP	UDP	Media/speech traffic. Depending on the customer network architecture, these ports might have to be opened in addition to the range in section 1.

					Ports within this range are randomly allocated when the call is set up
Media5 / Google ntp.media5corp.com, (time.google.com.) time1.google.com 216.239.35.0 time2.google.com 216.239.35.4 time3.google.com 216.239.35.8 time4.google.com 216.239.35.12	Outgoing	123	NTP	UDP	Time synchronization for Mediatrix devices
1.3 Cisco SPA112, ATA 191					
Tele2 213.100.32.64/27 213.100.32.240/28 213.100.33.0/28	Incoming* Outgoing	16384 - 16482	(S)RTP/RTCP	UDP	Media/speech traffic. Depending on the customer network architecture, these ports might have to be opened in addition to the range in section 1. Ports within this range are randomly allocated when the call is set up
0.ciscosb.pool.ntp.org**	Outgoing	123	NTP	UDP	Time synchronization.
1.4 Konftel 300IPx					
Konftel zti.konftel.com**	Outgoing	443	HTTP(S)	TCP	Konftel device settings distribution via the supplier's redirection system
Konftel upgrade.konftel.com**	Outgoing	80	HTTP	TCP	Firmware repository for Konftel devices
Konftel pool.ntp.org**	Outgoing	123	NTP	UDP	Time synchronization for Konftel 300IPx devices
Tele2 213.100.32.64/27 213.100.32.240/28 213.100.33.0/28	Incoming* Outgoing	4000 - 4008	(S)RTP/RTCP	UDP	Media/speech traffic. Depending on the customer network architecture, these ports might have to be opened in addition to the range in section 1. Ports within this range are randomly allocated when the call is set up
1.5 Snom devices					
Tele2 tele2vaxel.se 213.100.32.64/27 213.100.32.240/28 213.100.33.0/28	Outgoing	9443	HTTPS	TCP	Downloading provisioning settings for Snom devices
Snom downloads.snom.com**	Outgoing	80	HTTP	TCP	Firmware repository for Snom devices

1.6 Yealink W52P, W53P					
Tele2 213.100.32.64/27 213.100.32.240/28 213.100.33.0/28	Incoming* Outgoing	11780 - 11800	(S)RTP/RTCP	UDP	Media/speech traffic. Depending on the customer network architecture, these ports might have to be opened in addition to the range in section 1. Ports within this range are randomly allocated when the call is set up. Default is 11780 RTP / 11781 RTCP
cn.pool.ntp.org** time.windows.com**	Outgoing	123	NTP	UDP	Time synchronization for Yealink W52P and W53P. cn.pool.ntp.org is primary, time.windows.com is secondary.
1.7 Fanvil PA2					
Tele2 213.100.32.64/27 213.100.32.240/28 213.100.33.0/28	Incoming* Outgoing	10000 - 10200	(S)RTP/RTCP	UDP	Media/speech traffic. Depending on the customer network architecture, these ports might have to be opened in addition to the range in section 1. Ports within this range are randomly allocated when the call is set up.
time.nist.gov** pool.ntp.org**	Outgoing	123	NTP	UDP	Time synchronization for Fanvil PA2. Time.nist.gov is primary, pool.ntp.org is secondary

* If NAT is used in the network, it is commonly not needed to open for incoming traffic.
** For some hosts where Tele2 is not in control of the service provided, Tele2 cannot reliably provide the underlying IP addresses as they might change over time. See more information under “How do I find out the IP-address for a DNS hostname?”

2 Provisioning Mitel SIP desk phones

Every phone has a unique identifier, called MAC address.

Tele2 will preconfigure this address in the phone supplier's redirection service.
Upon first start, the phone contacts the redirection service and gets directed to Tele2.

When the phone is registered in Tele2s platform, Tele2 assigns it to a user and selects preferred firmware. Next time the phone is restarted or at a specific time interval it will download firmware and settings files automatically.

This provisioning procedure is only used for new phones. Once configured the phones will connect directly to Tele2, which will distribute future firmware updates and settings files.

2.1 Mitel 6800 startup sequence

When the phones are first unboxed, they are preconfigured with generic settings, not controlled by Tele2.
The phones first perform DHCP and LLDP. Then they contact the NTP servers specified under 1.1 Mitel devices to set the device time and date, enabling the security certificates to work properly. After that, the phones contact rcs.aastra.com to perform an initial firmware update and configuration files redirecting the phone to the correct customer in Tele2s systems based on MAC address. If no configuration exist in the RCS the phone will retry a few times and then lock down the auto-configuration functionality. If this happens the phone can be factory reset to enable the functionality again.

3 DHCP

All equipment relies on a customer network DHCP server to assign IP addresses, DNS server addresses and similar basic network configuration. This is noteworthy for example when devices are installed in a former "telephony network" or other solutions for separating IP telephony equipment from other network resources, as this needs to be routed to access the Internet and the required hosts and ports mentioned in the chapter Customer Firewall/CPE settings.

DHCP options and LLDP

Many IP devices support some LLDP functionality or DHCP options for providing control of different functionality, DHCP option 66 is for example a common way to control where the device tries to fetch configuration information, but other options can affect devices as well.

When migrating from or having the Tele2 Växel solution co-exist with other communication platforms, the network might have DHCP options in place for sending IP devices to internal configuration servers, or for example to the other PBX solution. LLDP might be used for directing certain equipment to a VLAN or similar.

These kinds of automatic control of devices might prevent any auto-provisioning or auto-configuration functionality in place to direct devices to Tele2 Växel, as well as making devices connect to internal network destinations instead of the Internet, and the general recommendation is to remove such DCHP options from the network prior to the installation of new devices with Tele2 Växel.

Signalling explained

In order to understand the different types of connections and firmware settings, we are describing the most common scenarios below.

Normal call

The phone call is set up through SIP messages using port 5061 (secure).

When the call is answered a random port from 49152 to 65534 is used for the media stream. Status- and indication messages (call clearing, DTMF) are sent and received using the SIP port.

Time settings

The Tele2 Växel PC apps will fetch the current time from Tele2's NTP server. This is normally performed during start up but also during up time within a specific interval.

For hardware devices, third party NTP servers are used for setting the local time in the device. This is important as the time must be correct during authentication.

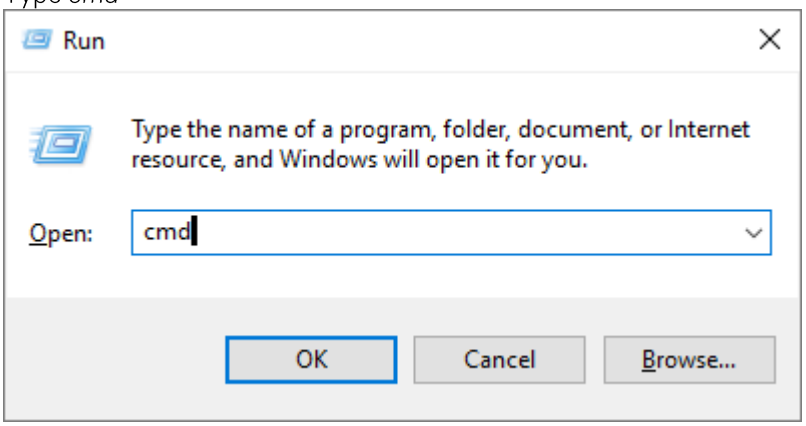
If traffic can't be allowed to the third party servers, an option available for most devices is to add DHCP option 42 in the network and use a local NTP server instead.

How do I find out the IP-address for a DNS hostname?

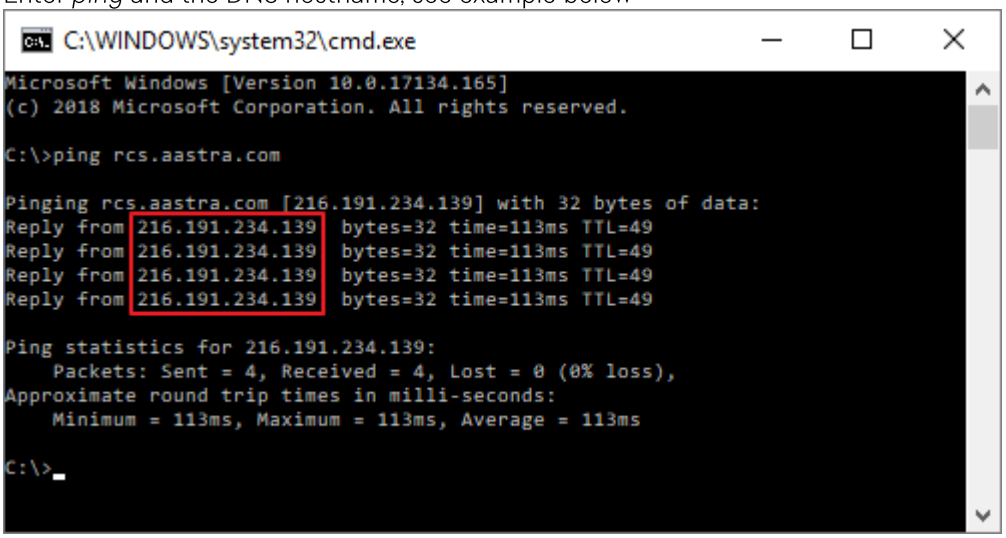
Many devices connect to servers outside Tele2 systems, e.g. for time synchronization or initial configuration. Tele2 doesn't always get updates on changes in the network structure and IP-addresses for those servers. If the customer network for example is restricting access to common services like NTP and HTTPS servers and cannot allow traffic to a DNS hostname, the current IP address for the servers in question can be obtained by the following method:

1. Press  +

2. Type *cmd*



3. Enter *ping* and the DNS hostname, see example below



4. Run the *ping hostname* multiple times to increase the possibility to find out if there currently are different addresses behind the hostname, for example due to load-balancing or geographic redundancy.

There are web based "whois" services available, that can provide more extensive information.