Tele2 Växel

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 other services based on the same platform.

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 network and firewall always has the correct settings.

For whom is this document?

This instruction is aimed at personnel with sufficient knowledge in configuring the company firewall and network settings

Update February 2024

Removed unused Tele2 NTP servers.
Added info for Microsoft Exchange integration.

Update December 2023

The firmware repository server for desk phones is moving to a new hosting environment and gets a new hostname. For the new server, firmware download is done via https port 443.

The new hostname is:
fw.tele2vaxel.se, 90.139.98.102

More servers added in the Grandstream GDMS device management platform.

Update April 2020

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

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 213.100.32.64/27 213.100.33.0/28	Outgoing	443	HTTPS	TLS	Web services, e.g. downloading software using secure HTTP,
Tele2 tele2vaxel.se 213.100.32.64/27 213.100.33.0/28	Incoming	443	HTTPS	TLS	Microsoft Exchange calendar integration
Tele2 tele2vaxel.se 213.100.32.64/27 213.100.33.0/28	Incoming* Outgoing	5061	SIP(S)	TLS	Signalling between Tele2 and connected devices. SIP inspection / SIP ALG should be disabled in the firewall
Tele2 tele2vaxel.se 213.100.32.64/27 213.100.33.0/28	Incoming* Outgoing	49152 - 65535	(S)RTP/RTCP	UDP	Media/speech traffic for Mitel 6800 devices, Tele2's user portal and other IP devices, and when the Tele2 Växel platform initiates the call to any device. Ports within this range are randomly allocated when the call is set up.
Dstny 185.39.124.98 185.39.124.99 185.39.125.98 185.39.125.99 185.39.125.17	Outgoing	443	HTTPS	TLS	The user portal is a web application that connects to the service over https for API requests and SIP via WSS.
1.1 Mitel devices					
Mitel rcs.aastra.com**	Outgoing	80/443	HTTPS	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
Tele2 fw.tele2vaxel.se 90.139.98.102	Outgoing	443	HTTPS	TLS	Firmware repository for Mitel devices

1.2 Grandstream HT801 – Tele2 VoIP Företagsabonnemang					
Tele2 213.100.32.64/27 213.100.33.0/28	Incoming* Outgoing	5004-5005	(S)RTP/RTCP	UDP	Media/speech traffic. Depending on the customer network architecture, traffic on these ports might have to be considered for calls initiated by the device, in addition to the range in section 1. Ports within this range are randomly allocated when the call is set up.
Grandstream eu.gdms.cloud 3.71.171.8	Outgoing	443	HTTPS	TCP	GDMS web portal, firmware download, & provisioning endpoints
Grandstream euacs.gdms.cloud 3.71.171.8 3.74.38.203 3.73.240.134	Outgoing	80 443	HTTP HTTPS	TCP	Communication between device and server
Grandstream acs-guest-a.gdms.cloud acsguesta.gdms.cloud 66.42.104.174 149.28.90.168 149.28.91.101 45.63.53.106	Outgoing	80 443	HTTP HTTPS	TCP	Communication between device and server
Grandstream eu.stun1.gdms.cloud 52.28.7.85 45.32.153.68	Outgoing	3478 3479		UDP	STUN, Keep-Alive, Client UDP packet reception
Grandstream stun-guest-a.gdms.cloud 45.63.104.45 207.246.119.209	Outgoing	3478 3479		UDP	Communication between device and server
Grandstream eu.syslog.gdms.cloud 52.28.7.85	Outgoing	6514		TCP	Communication between device and server
Grandstream eu.download.gdms.cloud 217.69.12.50	Outgoing	80 443	HTTP HTTPS	TCP	Firmware download and network speed detection
pool.ntp.org**	Outgoing	123	NTP	UDP	Time synchronization
1.3 Mediatrix 4102S, C710, C711 and S7 series					
Tele2 213.100.32.64/27 213.100.33.0/28	Incoming* Outgoing	5004 – 5134	(S)RTP/RTCP	UDP	Media/speech traffic. Depending on the customer network architecture, traffic on these ports might have to be considered for calls initiated by the device, 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
1.4 Cisco SPA112, ATA 191					
Tele2 213.100.32.64/27 213.100.33.0/28	Incoming* Outgoing	16384 - 16482	(S)RTP/RTCP	UDP	Media/speech traffic. Depending on the customer network architecture, traffic on these ports might have to be considered for calls initiated by the device, 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.
1.5 Konftel 300IPx					
Konftel zti.konftel.com**	Outgoing	443	HTTPS	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 213.100.32.64/27 213.100.33.0/28	Incoming* Outgoing	4000 - 4008	(S)RTP/RTCP	UDP	Media/speech traffic. Depending on the customer network architecture, traffic on these ports might have to be considered for calls initiated by the device, in addition to the range in section 1. Ports within this range are randomly allocated when the call is set up
1.6 Snom devices					
Tele2 tele2vaxel.se 213.100.32.64/27 213.100.33.0/28	Outgoing	9443	HTTPS	TCP	Downloading provisioning settings for Snom devices
Snom downloads.snom.com**	Outgoing	80	HTTP	TCP	Firmware repository for Snom devices

1.7 Yealink W52P, W53P					
Tele2 213.100.32.64/27 213.100.33.0/28	Incoming* Outgoing	11780 - 11800	(S)RTP/RTCP	UDP	Media/speech traffic. Depending on the customer network architecture, traffic on these ports might have to be considered for calls initiated by the device, 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.
1.8 Fanvil PA2					
Tele2 213.100.32.64/27 213.100.33.0/28	Incoming* Outgoing	10000 - 10200	(S)RTP/RTCP	UDP	Media/speech traffic. Depending on the customer network architecture, traffic on these ports might have to be considered for calls initiated by the device, 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 the device is connected to the Internet using NAT, it is commonly not needed to consider incoming traffic as that is handled automatically by the router. If the network requires opening for incoming traffic to the device, you as a customer are responsible for ensuring that devices are never directly accessible from the Internet for any web or control protocols. Failure to implement this will expose the device to intrusion attempts.
** 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 Network deployment

2.1 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.

2.1.1 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.

2.2 Dimensioning and performance

When calculating the network requirements for a user in the service, a measure of 80 kbit/s per simultaneous call can be used. The bandwidth differs depending on which codec that is used for the call. The Tele2 Växel Softphone sends/receives some HTTPS traffic periodically even when idle, such as for updating call queue status information in the user interface.
To ensure a well-functioning telephony service, the network should meet the following requirements:

- Packet loss must not be more than a maximum of 1%
- According to ITU G.114, End-to-End delay (mouth to ear) must not be greater than 150 ms
- Jitter, ie the difference in transmission time between the IP packets must be < 25 ms.

2.2.1 Codecs

These are examples of common codecs for different call scenarios. Additional codecs may occur, and the available codecs are subject to change.

To/From	To/From	Codecs
Mobile/external network	Softphone Mitel SIP phone 3rd party SIP phone	PCMA (G711a) AMR AMR WB (standard when on-net)
Softphone	Softphone	Opus
Mitel SIP phone	Softphone	PCMA (G711a)
3rd party SIP phone	Softphone	PCMA (G711a) Other codecs (such as Opus) are possible based on the 3rd party phone capabilites
3rd party SIP phone	Mitel SIP phone	PCMA (G711a)
Business Trunk	Softphone	PCMA (G711a)

Business Trunk	Mitel SIP phone	PCMA (G711a)
Business Trunk	3rd party SIP phone	PCMA (G711a)

2.3 Prioritization

Depending on network load and network architecture, it may be required to prioritize voice traffic to provide a good user experience. Different user endpoints have different capabilities and prerequisites regarding prioritization of traffic.

- Incoming voice traffic from the Tele2 Växel platform towards user endpoints is marked with DSCP class AF31 for SIP and EF for RTP.
- Tele2 Växel Softphone does not mark outgoing traffic in any way, if prioritization of outgoing traffic is desired, this can be achieved in the computer by an AD policy.
- For different hardware devices, traffic may be marked based on the supplier's settings, and may be possible to adjust in the device's management interface. For the Mitel phones that are managed by the Tele2 Växel service, outgoing traffic is marked with DSCP class AF31 for SIP and EF for RTP.

In addition, voice traffic can be prioritized based on IP addresses, all voice traffic is transmitted via the host addresses described in section 1. Customer Firewall/CPE settings.

3 Signalling explained

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

3.1 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 assigned for the media stream in the SDP.

Status- and indication messages (call clearing, DTMF) are sent and received using the SIP port.

All calls are routed through the Tele2 Växel service, no peer-to-peer-traffic occurs.

3.2 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.

3.3 Certificate

The platform uses a public certificate for encryption of traffic.
If a device validates root certificates, it must support the following chain of trust:

AddTrust External CA Root

USERTrust RSA Certification Authority (Intermediate)

Sectigo RSA DV/OV/EV Secure Server CA

End Entity [Leaf Certificate]

3.4 TLS

All communication with the Tele2 Växel platform must take place over the transport protocol TLS 1.2 or TLS 1.3 and the device must support Forward Secrecy.

What is TLS? Transport Layer Security or TLS is one of the world's most widely used encrypted communication protocols. The name suggests that TLS is used in the so-called transport layer in a connection. In a connection with TLS, many types of secure encrypted communication can be carried out, e.g., HTTP(S) for web pages and SIP(S) for media sessions (including phone and video calls) - then often in communication with SRTP for encrypted media streams during the session (conversation). In the Tele2 Växel platform, SRTP is also an absolute requirement. TLS has existed in several versions, with most of the equipment sold today supporting version 1.2. TLS version 1.3 is the latest version. The previous versions 1.0 and 1.1 are considered insecure today.

3.5 Connection details

The external address of the Tele2 Växel platform is tele2vaxel.se, which is accessible via public Internet.
For routing to the Customer's organization within the Tele2 Växel platform, the organization's domain name in the platform is used.

In SIP devices the external address is usually stated in configuration fields such as Outbound Proxy or Proxy, and the Customer domain name in fields such as: Proxy, SIP Registrar, SIP Server and the like, depending on the device.

In the PBX platform, every user has a username automatically assigned by Tele2s systems. The format for the username is u14901104 or similar. The username is used as sip.User in signaling
In addition, the main phone number of the subscription is set as a separate identifier for simplifying login. The identifier is typically the mobile number (+467), for users that only have a fixed line number, that is used instead.

3.5.1 Connecting a third-party SIP device

The service only accepts connections via the username for user endpoints managed by the service itself. For connecting third-party devices, a separate SIP account can be activated. This account has an automatically generated username with the format device.username@customerdomain.se.
In most SIP devices, only device.username is entered in the username fields in the account configuration.
The password entered in the device is a separate password for the third-party SIP account and not the password that the user may log in with in the web interface at tele2vaxel.se.

Many devices need to be set to accept SRTP in the signaling during the set of the call. It is often achieved by setting the setting of SRTP to "Optional". The setting is often found in a menu called Voice, RTP, Media, Audio, or similar.

4 SIP devices

Tele2 provides limited support for a selection of SIP terminals of various types. These are kept tested and verified for compatibility with Tele2 services. Tele2 cannot guarantee a certain functionality over time, but our ambition is to be able to notify about changes in compatibility if this happens. For example:

- that a phone or other hardware stops working with a service because its manufacturer no longer updates it to support modern security requirements or the communication methods and voice codecs that are supported in the service.
- that a phone or other hardware needs to be upgraded to a new firmware to continue working or to maintain a reasonable level of security.
- that a phone or other hardware loses certain functionality e.g., when changing the service, or when the hardware is upgraded to a firmware required to continue working in the service.

For information on which terminals are recommended for the Tele2 Växel platform at any given time, please contact Tele2 Customer Service.

Tele2 is not responsible for the compatibility of terminals with peripherals at the customer, such as intercoms, fax machines, speaker systems, headsets and the like. Tele2 can work with troubleshooting and adaptation of configuration according to the current Tele2 Additional work price list.

If you as a customer have terminals of Tele2 recommended or other models and want to connect them to the Tele2 Växel platform, it is often possible to implement. However, we would like to clarify the following:

- Tele2 does not handle returns, warranty commitments or repairs for equipment that is not purchased from Tele2.
- For terminals that are not sold by Tele2 or for questions that are related to the customer's computer network or internet connection, guidance and troubleshooting is carried out only according to best effort.
- You as a customer are responsible for using terminals and firmware in these that provide an adequate level of security in addition to the minimum requirements that exist at any given time for connection to the platform.

In many cases, phones and other hardware are supplied pre-configured from Tele2's distributors and can be connected and used directly. In other cases, Tele2's delivery department or customer service will help with account information, but the customer will be responsible for ensuring that the terminals are set up correctly and can be connected to the platform.

4.1 Mitel SIP desk phones provisioning

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.

When the phone is first unboxed, it is preconfigured with generic settings, not controlled by Tele2. The phone first performs DHCP and LLDP. Then it contacts 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 phone contacts rcs.aastra.com to perform an initial firmware update and to get configuration files redirecting the phone to the correct customer in Tele2s systems based on MAC address. If no configuration exists in the RCS, the phone will retry a few times and then lock down the auto-configuration functionality. If this happens the phone must be factory reset to enable the functionality again.

4.2 Grandstream HT801

Every device has unique identifiers: a MAC address and a serial number.

When the VoIP Företagsabonnemang subscription is ordered, Tele2s systems automatically preconfigures the device identifiers in the device supplier's redirection service, along with the SIP connection details.
Upon first start, the device contacts the redirection service and gets directed to Tele2.

When the device is first unboxed, it is preconfigured with generic settings, not controlled by Tele2. The device first performs DHCP. Then it contacts the NTP server specified under 1.2 Grandstream HT801 – Tele2 VoIP Företagsabonnemang to set the device time and date, enabling the security certificates to work properly.

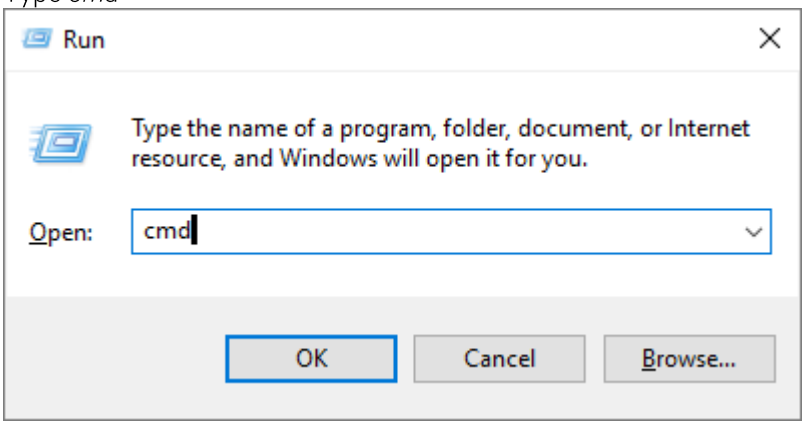
After that, the device contacts Grandstream GDMS to perform an initial firmware update and to get configuration files with the necessary settings to connect to and work properly with Tele2s platform.
During normal use, the device performs periodical check-ins with the GDMS service to get new configuration parameters and firmware updates as specified by Tele2, without customer involvement. It is important to ensure that the device is allowed to connect to GDMS in the network where it is connected, to ensure proper functionality over time.

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

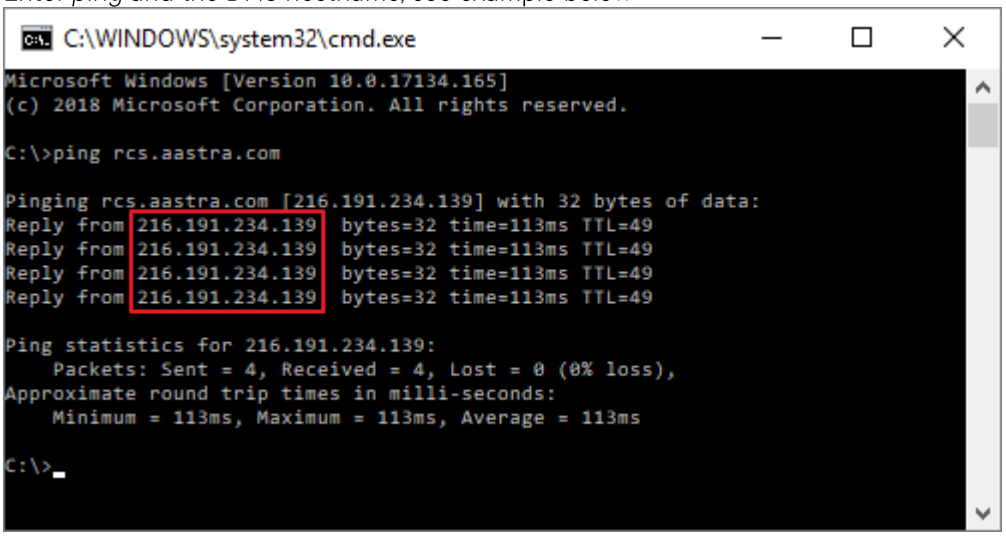
Many devices connect to servers outside Tele2 systems, e.g., for time synchronization or initial configuration. Tele2 doesn't always get updates on changes in the network structure and IP-addresses for those servers and therefore the information on IP addresses for such systems are not provided in this document. If the customer network for example is restricting access to common services like NTP and HTTPS servers and cannot allow traffic to a FQDN/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 may provide more extensive information.