Microsoft Teams with Direct Routing

February 2, 2021
# Microsoft Teams with Direct Routing

## Contents

1. **Introduction** .................................................................................................................. 5
2. **Requirements** ................................................................................................................. 6
3. **Microsoft Teams Direct Routing** .................................................................................. 7
   3.1 Connect to Office365 via PowerShell ............................................................................ 8
   3.2 Pair the anynode Software SBC to the Tenant .......................................................... 9
   3.3 Verify the anynode Software SBC Pairing ................................................................. 9
   3.4 Enable Users for Direct Routing ............................................................................... 10
   3.5 FQDNs, IP Addresses and Port Ranges .................................................................... 12
4. **anynode** ....................................................................................................................... 13
   4.1 Abstract Processing Overview .................................................................................. 13
   4.2 Wizard ....................................................................................................................... 14
   4.3 Guided Setup for Microsoft Teams Direct Routing ................................................ 15
      4.3.1 Microsoft Teams Direct Routing Node ............................................................. 16
         4.3.1.1 Microsoft Teams ......................................................................................... 16
         4.3.1.2 Network Controller .................................................................................... 17
         4.3.1.3 Ports ............................................................................................................ 17
         4.3.1.4 Certificate & Private Key ............................................................................ 18
         4.3.1.5 Certificate Chain .................................................................................... 20
         4.3.1.6 SBC FQDN ................................................................................................. 20
         4.3.1.7 Routing Domains ...................................................................................... 21
         4.3.1.8 Name ......................................................................................................... 21
      4.3.2 Voice over IP Provider Node .............................................................................. 23
      4.3.3 Routing ............................................................................................................. 30
   4.4 Validate the Connectivity via SIP Options .................................................................. 31
   4.5 Routing Domains ......................................................................................................... 32
   4.6 Microsoft Teams Node Details .................................................................................... 33
      4.6.1 SIP Node ........................................................................................................... 33
      4.6.2 SIP Transport ................................................................................................... 34
      4.6.3 Network Peer Whitelist .................................................................................... 35
      4.6.4 Network Controller .......................................................................................... 36
      4.6.5 Network Security Profile .................................................................................. 37
   4.7 Dashboard ..................................................................................................................... 38
   4.8 Example: Dial String Manipulations .......................................................................... 39
   4.9 Example: Multiple Tenants (Non-Carrier Trunk) ...................................................... 40
   4.10 Considerations for Media Bypass ............................................................................. 42
   4.11 License ....................................................................................................................... 46
Microsoft Teams with Direct Routing

5 Using a Microsoft Teams Direct Routing Carrier Trunk

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Microsoft Teams Carrier Tenant</td>
<td>50</td>
</tr>
<tr>
<td>5.2 Microsoft Teams Customer Tenants</td>
<td>52</td>
</tr>
<tr>
<td>5.3 Guided anynode Setup</td>
<td>55</td>
</tr>
<tr>
<td>5.3.1 Additional Customer Tenant Nodes</td>
<td>62</td>
</tr>
<tr>
<td>5.3.2 Tenant FQDN</td>
<td>65</td>
</tr>
<tr>
<td>5.3.3 SBC FQDN</td>
<td>66</td>
</tr>
<tr>
<td>5.3.4 Microsoft Teams Connectivity</td>
<td>67</td>
</tr>
<tr>
<td>5.3.5 SIP Domain</td>
<td>68</td>
</tr>
<tr>
<td>5.3.6 Routing Domains</td>
<td>69</td>
</tr>
</tbody>
</table>

6 E911 Dynamic Emergency Calls with Microsoft Teams

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1 Example: anynode with an E911 Provider</td>
<td>71</td>
</tr>
<tr>
<td>6.1.1 Routing Domain</td>
<td>71</td>
</tr>
<tr>
<td>6.1.2 Routing Forward Profile</td>
<td>72</td>
</tr>
<tr>
<td>6.1.3 SIP User Agent - RFC 6442</td>
<td>73</td>
</tr>
<tr>
<td>6.1.4 SIP User Agent - Processing SIP Geolocation ELIN URI</td>
<td>74</td>
</tr>
<tr>
<td>6.2 Plan and Configure Dynamic Emergency Calling for Microsoft Teams</td>
<td>75</td>
</tr>
<tr>
<td>6.3 Test and Check Geolocation and E911 Related Emergency Call Headers</td>
<td>77</td>
</tr>
</tbody>
</table>

7 Local Media Optimization with anynode and Microsoft Teams

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1 Microsoft Teams Tenant with Local Media Optimization</td>
<td>81</td>
</tr>
<tr>
<td>7.2 Guided anynode Setup for Local Media Optimization</td>
<td>84</td>
</tr>
<tr>
<td>7.2.1 Setting up the Site SBC Node for the anynode Proxy SBC</td>
<td>92</td>
</tr>
<tr>
<td>7.2.1.1 Set the Site SBC FQDN for anynode's Proxy SBC Node</td>
<td>96</td>
</tr>
<tr>
<td>7.2.2 anynode Site SBC Configuration</td>
<td>98</td>
</tr>
</tbody>
</table>

8 Appendix

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1 Test Call</td>
<td>105</td>
</tr>
<tr>
<td>8.2 Active Sessions</td>
<td>105</td>
</tr>
<tr>
<td>8.3 Call History</td>
<td>106</td>
</tr>
<tr>
<td>8.4 Tracing</td>
<td>107</td>
</tr>
<tr>
<td>8.5 Trace Analyzer</td>
<td>108</td>
</tr>
<tr>
<td>8.6 Trial Version</td>
<td>109</td>
</tr>
<tr>
<td>8.7 Hosted in Microsoft Azure</td>
<td>110</td>
</tr>
<tr>
<td>8.8 anynode Installation</td>
<td>111</td>
</tr>
<tr>
<td>8.9 Information, License and Support Requests</td>
<td>112</td>
</tr>
</tbody>
</table>
Introduction

anynode® is a Microsoft Teams certified Session Border Controller that is entirely a software based solution. It will work as an interface for numerous SIP Endpoints like SIP phones, SIP PBXs and SIP carriers. It converts port and directory information, provides higher security, routes session traffic and does manipulation of call numbers.

This document is intended to support you with the integration and configuration of anynode to leverage SIP trunking for allowing Direct Routing and enabling on-premise PSTN connectivity for Microsoft Teams clients. The following sections describe the essential configuration steps for that. Please refer to the respective manufacturer documentations and manuals for detailed Microsoft Teams installation, deployment and configuration procedures. For in-depth details regarding Direct Routing, please take a closer look at the Plan Direct Routing and Configure Direct Routing sections of the MS Teams documentation.

Additional anynode information and documents (TechNotes) can be found on our website https://www.anynode.de or YouTube channel where you can also find the Connect Microsoft Teams Direct Routing video.

For anynode related information and details, for e.g.: system requirements, performance, features, routing, manipulations, security, high availability considerations, anynode tools, please check with:

- anynode
- anynode’s YouTube Channel
- Community
- anynode with Microsoft Teams
- anynode’s Data Sheet
- anynode’s Interoperability List
Requirements

1. An Office 365 tenant that is used for the Microsoft Teams users homed in Office 365 with the required configuration and connection to anynode (sfb.te-systems.com in this example).

2. Microsoft Teams users that are enabled direct routing and licensed for Office 365 Phone System (E5 or E1/E3 with Office 365 Phone System add-on). For Microsoft Teams infrastructure and license requirements please check with the manufacturer given Plan Direct Routing information.

3. A public and reachable IP address and public DNS entry with proper mapping for the anynode server (sbc1.sfb.te-systems.com for the standard pairing example). Take note that the anynode server must be reachable through the public IP network. A fully Qualified Domain Name (FQDN) for anynode and its server where the domain portion of the FQDN has to be registered in the Direct Routing configurations of the Office 365 tenant. Check that the FQDN and public DNS entries resolve correctly to the proper IP address. Please note that you are not allowed using Microsoft's automatically created tenant domain *.onmicrosoft.com for the FQDN of the anynode server.

4. A public trusted certificate is needed for communication between anynode and Microsoft's Direct Routing cloud service. This certificate must be generated by one of Microsoft's accepted root certificate authorities for Direct Routing. Please note that the certificate needs to have anynode’s FQDN in the subject, common name, or subject alternate name fields. For details please check with the Public trusted certificate for the SBC section given in Microsoft’s Plan Direct Routing documents.

5. Even with the description in the Microsoft documents, we are frequently asked about the topics SIP Signaling: FQDNs and firewall ports and Media traffic: Port ranges. Because of this, we will give a brief overview in the corresponding chapter on page 12.

6. At least an anynode installation using the certified version 3.20 (or higher). Please note, Microsoft Teams Carrier Trunks require using anynode version 4.0!

7. Appropriate network access, network routing and administration rights.

8. Accessible, installed and configured VoIP environment.

9. VoIP credentials for the involved nodes to allow for appropriate configurations.

10. A full or trial anynode license. Please request a trial license from our sales team or contact them for any license related questions or general questions about our products. Some more details can be found in the chapter Information, License and Support Requests on page 112.
Microsoft Teams Direct Routing

As a pre-requisite, all preliminary administrative configurations for the Microsoft Phone System environment have to be completed. This includes network and cloud related configurations. An example of this is accessing Microsoft's cloud service via PowerShell. Check to make sure that the administrative account and Microsoft Windows set up is able to access the cloud via PowerShell and that the appropriate cmdlets can be invoked for proper configurations. To enable the Direct Routing services for the appropriate Teams users, you must configure anynode as a session border controller in the Microsoft Phone System environment. Before we start with the anynode configuration for our example, we give a brief overview of the corresponding Microsoft Teams Direct Routing set up.

For further details, please continue to check the following Microsoft documentation on a regular basis, since this content is still subject to change at the time of writing this TechNote.

- Microsoft Teams Phone System Direct Routing overview
- Set up your computer for Windows PowerShell and for troubleshooting with its related Diagnose connection problems with the Skype for Business Online Connector topics.
- Plan Direct Routing
- Configure Direct Routing
- Configure a Session Border Controller for multiple tenants

Enabling, creating or moving users for Direct Routing Service and making sure they are homed for Skype for Business Online is beyond the scope of this document. The same goes for Voice Routing configurations with its policies, dial plan handling and PSTN usage. For information on these, refer to the corresponding Microsoft documentation.
3.1 Connect to Office365 via PowerShell

The PowerShell session connected to the tenant for pairing the anynode software SBC to the Direct Routing interface is shown below. For details about this please check the appropriate Microsoft docs Set up your computer for Windows PowerShell. Note: The Windows PowerShell credential request for the User is not shown in detail here.

```powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\> Import-Module SkypeOnlineConnector
PS C:\> $teamsSession = New-CsOnlineSession -UserName support@te-systems.de
PS C:\> Import-PSSession $teamsSession -AllowClobber
ModuleType Version Name ExportedCommands
---------- ------- ---- ----------------
Script 1.0 tmp_4dpzx6ax.lsm (Clear-CsOnlineTelephoneNumberReservation, Complete-Cs...
```

As recommended in the Microsoft documentation you may want to check the command availability for being able to set up anynode as session border controller via the **CsOnlinePSTNGateway** cmdlet as shown here.

```powershell
PS C:\> Get-Command *onlinePSTNGateway*
CommandType Name Version Source
----------- ---- ------- -----
Function Get-CsOnlinePSTNGateway 1.0 tmp_kfqua10c.eos
Function New-CsOnlinePSTNGateway 1.0 tmp_kfqua10c.eos
Function Remove-CsOnlinePSTNGateway 1.0 tmp_kfqua10c.eos
Function Set-CsOnlinePSTNGateway 1.0 tmp_kfqua10c.eos
```
3.2 Pair the anynode Software SBC to the Tenant

Before you start with the pairing, check the domains that have been configured for the Skype for Business Online tenants with the `Get-CsTenant` cmdlet. The domain in this example is `sfb.te-systems.com`.

```powershell
PS C:\> Get-CsTenant | fl Domains
Domains : [sfb.te-systems.com, TESYSTEMS365.mail.onmicrosoft.com, TESYSTEMS365.onmicrosoft.com]
```

Pairing anynode with the `New-CsOnlinePSTNGateway` cmdlet is shown here. anynode's FQDN is `sbc1.sfb.te-systems.com` and is using the `SipSignallingPort` port 5067, which is also set by default through anynode's assistant for the MS Teams scenario. The corresponding port configuration of anynode's Teams will be shown in the chapter `Ports` on page 17. Multiple `CsOnlinePSTNGateway`'s (ie: `sbc1.sfb.te-systems.com`, `sbc2.sfb.te-systems.com` etc.) and multiple voice routes can be defined for enabling high availability, fallback or voice route specific scenarios. Please note in the example below, Media Bypass is not enabled yet (MediaBypass: False). If you would like to make use of Media Bypass, we strongly recommend you review the chapter `Considerations for Media Bypass`, which can be found on page 42.

```powershell
PS C:\> New-CsOnlinePSTNGateway -Identity sbc1.sfb.te-systems.com
-SipSignallingPort 5067
-ForwardCallHistory $true
-MaxConcurrentSessions 100
-Enabled $true

Identity : sbc1.sfb.te-systems.com
Fqdn : sbc1.sfb.te-systems.com
SipSignallingPort : 5067
CodecPriority : SILKWB,SILKNB,PCMU,PCMA
ExcludedCodecs :
FailoverTimeSeconds : 10
ForwardCallHistory : True
ForwardPai : False
SendSipOptions : True
MaxConcurrentSessions : 100
Enabled : True
MediaBypass : False
```

3.3 Verify the anynode Software SBC Pairing

Check if anynode is now being listed as a paired session border controller via `Get-CsOnlinePSTNGateway` cmdlet. Ensure that the result of the `Enabled` parameter is True, which indicates that anynode is enabled and allowed for outbound calls.

```powershell
PS C:> Get-CsOnlinePSTNGateway

Identity : sbc1.sfb.te-systems.com
Fqdn : sbc1.sfb.te-systems.com
SipSignallingPort : 5067
CodecPriority : SILKWB,SILKNB,PCMU,PCMA
ExcludedCodecs :
FailoverTimeSeconds : 10
ForwardCallHistory : True
ForwardPai : False
SendSipOptions : True
MaxConcurrentSessions : 100
Enabled : True
MediaBypass : False
```
3.4 Enable Users for Direct Routing

For participation in the Direct Routing Service, the associated Office 365 users must be created and enabled. Those users must be homed in Skype for Business Online and being equipped with phone system license. The users must also be configured with proper phone number and voice routing configurations and enabled for enterprise voice and voicemail in accordance with the dial plan. The test user in this example is enabled for voicemail and configured with a full E.164 phone number as shown below. Please note that the displayed output is restricted to the most relevant parameters:

```
PS C:\> Set-CsUser -Identity "Bobby Bob" -OnPremLineURI tel:+4953638195108
-EnterpriseVoiceEnabled $true -HostedVoiceMail $true
PS C:\> Get-CsOnlineUser -Identity "Bobby Bob"

Description : {Newly created in AD}
Alias : Bobby
UsageLocation : US
OnPremEnterpriseVoiceEnabled : True
OnPremSIPAddress : sip:Bobby@sfb.te-systems.com
OnPremLineURI : tel:+4953638195108
HostedVoiceMail : True
DisplayName : Bobby Bob
EnterpriseVoiceEnabled : True
Enabled : True
VoicePolicy : HybridVoice
TeamsCallingPolicy : Global
TeamsUpgradePolicy : UpgradeToTeams
DialPlan : DE
OnlineVoiceRoutingPolicy : German TE

Grant to a voice routing policy for the user:

```
PS C:\> Grant-CsOnlineVoiceRoutingPolicy -Identity "Bobby Bob" -PolicyName "German TE"
```

Validate the policy assignment:

```
PS C:\> Get-CsOnlineUser -Identity "Bobby Bob" | select OnlineVoiceRoutingPolicy

OnlineVoiceRoutingPolicy
-----------------------
German TE
```

Check with the Get-CsOnlineUser cmdlet and verify if the user is homed in Skype for Business online and assigned to the appropriate HostingProvider and RegistrarPool parameters. Verify the users are assigned to the HostingProvider domain sipfed.online.lync.com and they are homed in the infra.lync.com domain for the RegistrarPool parameter.

```
PS C:\> Get-CsOnlineUser -Identity "Bobby Bob" | fl HostingProvider, RegistrarPool

HostingProvider : sipfed.online.lync.com
RegistrarPool : sippoolAM41E02.infra.lync.com
```

For a better overview about these displayed examples of user relations and configurations, additional information is shown next.

```
PS C:\> Get-CsOnlinePSTNUsage

Identity : Global
Usage : {Germany TE}
```
This example **CsOnlineVoiceRoute** is assigned as follows:

```powershell
PS C:\> Get-CsOnlineVoiceRoute
Identity : LocalRoute
Priority : 0
Description :
NumberPattern : ^\(+1\[0-9]\{10\}\)$
OnlinePstnUsages : {}
OnlinePstnGatewayList : {}
Name : LocalRoute
Identity : To +49
Priority : 1
Description :
NumberPattern : ^\+49\(\d\{3\,20\}\)$
OnlinePstnUsages : {GermanyTE}
OnlinePstnGatewayList : {sbc1.sfb.te-systems.com}
Name : To +49
```

This is an example of the **CsOnlineVoiceRoutingPolicy** which gets assigned to Direct Routing users. Verify that the corresponding **RouteType** is set.

```powershell
PS C:\> Get-CsOnlineVoiceRoutingPolicy
Identity : Global
OnlinePstnUsages : {}
Description :
RouteType :
Identity : Tag:German TE
OnlinePstnUsages : {GermanyTE}
Description :
RouteType : BYOT
```

This example **CsTeamsCallingPolicy** (Global Identity) is shown next. **AllowPrivateCalling** must be True to enable any calling features in Teams.

```powershell
PS C:\> Get-CsTeamsCallingPolicy
Identity : Global
AllowCalling : True
AllowPrivateCalling : True
Identity : Tag:AllowCalling
AllowCalling : True
AllowPrivateCalling : True
Identity : Tag:DisallowCalling
AllowCalling : False
AllowPrivateCalling : False
```

This example **CsTeamsUpgradePolicy** is used as shown next.

```powershell
PS C:\Users\Sascha> Get-CsTeamsUpgradePolicy
Identity : Global
Description : Users can use either Skype for Business client or Teams client
Mode : Legacy
NotifySfbUsers : False
Action : None
Identity : Tag:UpgradeToTeams
Description : Use Teams Only
Mode : TeamsOnly
NotifySfbUsers : False
Action : Upgrade
```
### 3.5 FQDNs, IP Addresses and Port Ranges

Before we discuss examples of Direct Routing configuration details, a brief overview about the relevant IP addresses and ports will be given. These addresses and ports have to be opened to allow for proper SIP and media signaling between the anynode environment and Microsoft's Teams cloud service. In addition to IP addresses and ports used by anynode's Direct Routing Node, you will need to review Microsoft's Plan Direct Routing documentation so the appropriate ports are opened to allow outbound and inbound connections. By default the anynode wizard sets port 5067 for SIP/TLS (which is also used for the tenant pairing in this scenario) and the port range 10000 - 13000 for UDP/SRTP media signaling what allows up to 1000 concurrent sessions. On demand, this range can be lowered through anynode's guided setup as described in the chapter **Ports** on page 17. Microsoft recommends utilizing at least two ports per concurrent call and use the following FQDNs:

- `sip.pstnhub.microsoft.com`
- `sip2.pstnhub.microsoft.com`
- `sip3.pstnhub.microsoft.com`

Please note: If DNS names are supported by the firewall, the FQDN `sip.all.pstnhub.microsoft.com` resolves all given IP’s. This FQDN’s will be resolved to one of these listed IP addresses:

- 52.114.148.0
- 52.114.132.46
- 52.114.75.24
- 52.114.76.76
- 52.114.7.24
- 52.114.14.70

For this FQDN’s and each of the above listed IP addresses the following ports must be opened for inbound and outbound SIP/TLS signaling:

<table>
<thead>
<tr>
<th>SIP Signaling From</th>
<th>SIP Signaling To</th>
<th>Source Port(s)</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Teams SIP Proxy</td>
<td>anynode Teams Node</td>
<td>1024 - 65535</td>
<td>5067</td>
</tr>
<tr>
<td>anynode Teams Node</td>
<td>Teams SIP Proxy</td>
<td>10000 - 13000</td>
<td>5061</td>
</tr>
</tbody>
</table>

Microsoft’s Direct Routing cloud service requires the following IP address and port range for processing the media data:

- 52.112.0.0/14 (IP address range from 52.112.0.1 to 52.115.255.254)

For this IP range the following UDP/SRTP ports must be opened for processing the media data:

<table>
<thead>
<tr>
<th>Media From</th>
<th>Media To</th>
<th>Source Port Range</th>
<th>Destination Port Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Cloud</td>
<td>anynode</td>
<td>49152 - 53247</td>
<td>10000 - 13000</td>
</tr>
<tr>
<td>anynode</td>
<td>Microsoft Cloud</td>
<td>10000 - 13000</td>
<td>49152 - 53247</td>
</tr>
</tbody>
</table>

The anynode related FQDN, IP and port settings can be reviewed in the **Microsoft Teams Node Details** chapter starting on page 33.
anynode

For enabling the communication between the Microsoft Teams Direct Routing and other nodes through anynode, those endpoints have to be configured as a Node. Each Node can handle several rules for incoming and outgoing numbering and dial string manipulations. Routing decisions can be made based on the source or destination prefix, extension ranges and on the source Node. If a call matches a filter rule, it will be routed to the configured destination Node. This document shows a basic configuration between Teams, a SIP Provider Node and anynode with some call number manipulations and routing table relations.

4.1 Abstract Processing Overview

Before the anynode configurations will be described in detail, an abstract overview about its processing topology will be given. Single or multiple Nodes (SIP or UCMA) can be defined for anynode. A Routing Domain is used for routing decisions between the nodes. Even though anynode can handle multiple routing domains, most scenarios function fine using only one routing domain.

An inbound connection to that Node will be processed through its SIP dial string manipulations for incoming SIP messages. Specific filter and routing decisions are defined in the Routes table of a Routing Domain. Examples of this could be: source Node restrictions or different matching conditions according to the source and destination dial strings. anynode is also able to use matching conditions based on diversion numbers or defined lookup directories. In addition to the filter and routing decisions, several advanced actions can be taken into account via the Route Establishment handling. For example: actions referring to the call behavior and state (like route a call, reject a call or parallel call), using additional forwarding profiles or even rewriting specific dial strings.

After the filter, routing decisions and specified actions, final manipulations of the source and destination dial string can be made with the SIP dial string manipulations for outgoing SIP messages.

All these definitions follow the first match method and all rules will be processed from top to bottom. That means, if a routing rule matches, further processing inside the route table will be stopped. The Node’s dial string manipulations are processed until they match, or no further rules will be found in the manipulation table.
4.2 Wizard

The anynode configuration can easily be created through the wizard. Depending on which scenario you select, the wizard will assist you in making the configuration easier.

Please note that any configuration changes must be committed. If using the anynode wizard the commitment has to be done after the guided configuration steps.
4.3 Guided Setup for Microsoft Teams Direct Routing

The configuration setup will be created through the anynode wizard. For doing this, we will use one of the pre-defined configurations that apply to the local topology. As for this document's subject, the example ...Microsoft Teams Direct Routing and a VoIP Provider will be selected. Use the Start button to run through the Node Interconnection Assistant configuration tasks.
4.3.1 Microsoft Teams Direct Routing Node

The assistant now starts with first Node configuration, the Microsoft Teams Direct Routing Node. This Node contains various default configurations which have to be adjusted. To set up the Node details click the Configure button.

4.3.1.1 Microsoft Teams

Select Microsoft Teams Direct Routing for the standard trunking model. For the carrier trunk model which use additional derived trunks for their customers tenants, please check with the chapter Using a Microsoft Teams Direct Routing Carrier Trunk starting on page 47.
4.3.1.2 Network Controller

Initially, the assistant requests the network related Node settings. Select Create new network controller, as none is available yet. Usually the given defaults work fine, but you may want to specify the Interface, IP Version and IP Address for a better overview. Ensure that reverse DNS Lookup stays enabled for the public interface as this is a requirement for SIP through TLS connections.

4.3.1.3 Ports

For inbound firewall rules, you may define a UDP and SIP TCP port range which restricts the number of ports used by anynode. The number of ports in this range should at least be three times higher than the number of maximum concurrent sessions on this Node. If multiple anynode Network Controllers share the same physical network interface of the host, make sure to select unique port ranges to avoid any port overlapping. Note that the Microsoft Teams Direct Routing SIP Node is set to port 5067 as this is the commonly used default of Microsoft’s phone system. The corresponding port configurations for the Direct Routing setup can be reviewed in the chapter Pair the anynode Software SBC to the Tenant from page 9.
4.3.1.4 Certificate & Private Key

Next, the private key and public certificate has to be set. To start click the Configure... button. Such configurations can be made, reviewed or changed anytime in the Network Security Profile dialog of the referring Node. Please note that the certificate needs to have the given SBC FQDN in one of the following fields: subject, common name or subject alternate name.

The required certificate and the private key will be imported via the Import of the certificate and/or private key option.
Both certificates have to be imported in single files. So both files have to be browsed to, selected and imported one at a time. If the import and subject validation is fine and nothing is highlighted red, you can proceed with **Finish**.

If everything is set for the **Certificate & Private Key** dialog, proceed with **Next**.
4.3.1.5 Certificate Chain

Next, the certificate chain is properly displayed as anynode provides some default validation certificates. If there is no valid chain available, the corresponding certificate has to be imported via the Add... button.

4.3.1.6 SBC FQDN

Next, anynode’s FQDN must be entered. If provided, the FQDN will be automatically determined through the previous given certificates. This FQDN is the one used for the SBC pairing with Office 365 tenant as shown and described in the chapter Microsoft Teams Direct Routing on page 7. This is the valid FQDN domain portion for the pairing. This FQDN is also statically mapped to the corresponding SIP, from and SIP contact headers, as external host name for the SIP Options packets that will be send by anynode. Thoroughly review the Microsoft documentation on Direct Routing configurations and their explanations.
4.3.7 Routing Domains

This dialog must be skipped for now as no routing domain exist yet. With a new setup, the initial Routing Domain will be set after running through anynode’s wizard. However, for an present anynode configuration with existing routing domains, select the required one.

4.3.8 Name

The last dialog sets a default name which can be renamed if needed. As usual click Finish to proceed.
The **Node Interconnection Assistant** gives an overview about the already performed configurations for this Node. If everything is correct, continue with **Next** to start the second Node configuration of the selected scenario.
4.3.2 Voice over IP Provider Node

For the Voice over IP Provider Node, anynode’s Node Interconnection Assistant sets various defaults for the selected scenario.

As mentioned in the introduction, a Voice over IP Provider is used in this example. For generalization reasons [Other VoIP Provider] is selected.
Like the first Node, the network related controller settings have to be set. Unless you want to use only one, select **Create new network controller** for this Node. The default controller name can be changed and the appropriate network interface selections, the IP Version, IP Address and Reverse DNS Lookup usage can be specified. If required or not supported, **Reverse DNS Lookup** can be disabled for this Node.

Again the port values for UDP, TCP and TLS can be assigned for this Voice over IP provider Node. Verify that the port values conform to all network and remote configurations.
As there are no NAT Traversal configurations required for this environment, we proceed with Next.

The SIP Interconnection type is here used with Node Interconnection via SIP trunking as no authentication credentials are needed for the Voice over IP provider.
Enter the SIP domain that is used by the remote site, the **Voice over IP Provider**.

The next configuration dialogs will be skipped as no authentication credentials and no proxy settings are required.
The **Asserted-URI** is set up on the provider requirements.

The **Network Peer List** for the provider Node sets some defaults. Hostnames or IP addresses can be added or changed as needed.
No incoming and outgoing dial string manipulations are required in this example. Regardless of this configuration, the chapter Example: Dial String Manipulations starting on page 39 gives a manipulation example.
Again a default Node name is set which can be changed according to your needs.

Now the Node Interconnection Assistant gives an overview about the already performed configurations. Proceed with Next to configure the Routing decision.
4.3.3 Routing

Use direct routing with prefix filter is used here for our routing method. This method routes the SIP session between both nodes if the given E.164 prefix matches. You may prefer the Use dial string routing method if the routing should be restricted to a specific dial string. The Use direct routing without prefix filter can be also used, but for security reasons it is not recommended at all. However, the configuration details of this method will be shown in the chapter Routing Domains starting on page 32.

Please note that the route selection occurs after the Incoming Manipulation and before the Outgoing Manipulation of the involved Node. Now, exit the assistant’s configuration tasks and get back to the main view of the anynode frontend by clicking Finish. Don’t forget to commit the newly configured scenario.
4.4 Validate the Connectivity via SIP Options

Please note that the Direct Routing cloud service only starts sending SIP options towards anynode’s configured CsOnlinePSTNGateway FQDN, after a SIP Option notification was properly received from this entity.

It must be verified that the initial SIP options notification of anynode delivers a valid FQDN through the SIP contact header.

The successful and failed SIP Option notifications can be checked in the Microsoft Teams Direct Routing Node in anynode’s Dashboard. For details about the Dashboard, check with the appropriate chapter on page 38. The SIP options can be reviewed through logs captured via anynode’s Trace Analyzer. More information about the Trace Analyzer will be given in the same chapter starting on page 108. However, an example of inbound and outbound SIP options with the correct 200 OK responses is given below. Take note that the given output of the following SIP messages has been shortened.

**SIP Options example from anynode to the Direct Routing Cloud Voice Phone System:**

```
OPTIONS sip:sip2.pstnhub.microsoft.com;lr SIP/2.0
Call-Id: c3553d1e-5038
Contact: <sip:sbc1.sfb.te-systems.com:5067;transport=tlscaddr=172.18.0.119>
Cseq: 320998504 OPTIONS
Supported: p-xz-siplb-load
To: <sip:sip2.pstnhub.microsoft.com;lr>

SIP/2.0 200 OK
Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, NOTIFY
Call-Id: c3553d1e-5038
Cseq: 320998504 OPTIONS
From: <sip:sbc1.sfb.te-systems.com:5067;transport=tlscaddr=172.18.0.119;tag=724a488f-9dc8>
Server: Microsoft.PSTNHub.SIPProxy v.2018.6.27.1 i.USWE2.4
Via: SIP/2.0/TLS 172.18.0.119:7513;branch=z9hG4bK51b2db71-e45b
```

**SIP Options example from the Direct Routing Cloud Voice Phone System to anynode:**

```
OPTIONS sip:sbc1.sfb.te-systems.com:5067;transport=tlscaddr=172.18.0.119 SIP/2.0
Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, NOTIFY
Call-Id: 63c3ce79-408b-44a7
Cseq: 1 OPTIONS
From: <sip:sip-du-a-us.pstnhub.microsoft.com:5061>
User-Agent: Microsoft.PSTNHub.SIPProxy v.2018.6.27.1 i.USWE2.4
Via: SIP/2.0/TLS 10.0.0.8:5061;received=52.114.148.0;branch=39hG4bK643f246

SIP/2.0 200 OK
Call-Id: 63c3ce79-408b-44a7
Cseq: 1 OPTIONS
From: <sip:sip-du-a-us.pstnhub.microsoft.com:5061;tag=2638721e-1a2e>
To: <sip:sbc1.sfb.te-systems.com:5067;transport=tlscaddr=172.18.0.119>
User-Agent: Microsoft.PSTNHub.SIPProxy v.2018.6.27.1 i.USWE2.4
Via: SIP/2.0/TLS 10.0.0.8:5061;received=52.114.148.0;branch=39hG4bK643f246
```
4.5 Routing Domains

As described in the previous chapter Routing, the routing domain entries with their filter and profile relations have been automatically created through the anynode wizard as follows.
4.6 Microsoft Teams Node Details

This chapter gives an overview of the most relevant anynode settings (FQDN'S, IP's, Ports) of the created MS Teams Node. All anynode configurations used here are the defaults of the wizard.

4.6.1 SIP Node

According to Microsoft’s Direct Routing specifications, the global main FQDN sip.pstnhub.microsoft.com is automatically set as Remote SIP Domain. The required FQDN's sip.pstnhub.microsoft.com, sip2.pstnhub.microsoft.com and sip3.pstnhub.microsoft.com are automatically set as transport connections, defined in the Microsoft Teams Direct Routing Node.
### 4.6.2 SIP Transport

Besides setting the public FQDN (here sbc1.sfb.te-systems.de) for anynode’s Microsoft Teams Direct Routing Node which needs to be set for SIP contact headers, the SIP/TLS default port 5067 and auto-created Network Peer Whitelist (as described in the same named chapter on page 35) are defined in the SIP Transport configurations.
4.6.3 Network Peer Whitelist

As mentioned in the chapter FQDNs, IP Addresses and Port Ranges on page 12, the anynode wizard automatically sets the sip-all.pstnhub.microsoft.com FQDN to the Network Peer Whitelist of the MS Teams Direct Routing Node.
4.6.4 Network Controller

anynode’s given default UDP port range for the Microsoft Direct Routing Node is defined within its Network Controller configurations.
4.6.5 Network Security Profile

You have to verify that the corresponding certificates, private keys and the validation certificate of your CA (certification authority) is set in the **Network Security Profile** of the **Microsoft Teams Direct Routing Node**. This was previously described in the **Microsoft Teams Node** configuration and the referring certificate section on page 18. As described before and shown on page 38 in the **Dashboard** chapter, check their states and validity.
4.7 Dashboard

anynode’s Dashboard gives an overview of various configuration states. Just switch the view to the Dashboard of anynode’s frontend Monitor Mode. A double-click onto a Node entry opens a new window with some more details. An example of the Microsoft Teams Direct Routing Node is shown on the screenshot below. The appropriate target URI’s sip.pstnhub.microsoft.com, sip2.pstnhub.microsoft.com and sip3.pstnhub.microsoft.com were automatically set through anynode’s scenario wizard and displayed as Transport Connections. The matching conditions, manipulations and targets are defined in the MS Teams SIP Node dialog as shown in the chapter on page 33. These entries can be changed as needed in the MS Teams Node.
4.8 Example: Dial String Manipulations

In the example below, which is quite common for German dial plans, adds prefix +4953638195 if any internal 3 digit extension number (Wildcard Pattern = "XXX") will be delivered. National or international numbers starting with prefix 0 and 00 will be normalized to an international based E.164 number with the + prefix. For more basics about dial string manipulations we recommend watching our YouTube video Basics Dial String Manipulation and Routing.
4.9 Example: Multiple Tenants (Non-Carrier Trunk)

Please note that this scenario is not recommended for SIP carrier trunks. For carrier trunks which use additional derived trunks for their customers tenants, please check with the chapter Using a Microsoft Teams Direct Routing Carrier Trunk starting on page 47 and the detailed Microsoft article Configure a Session Border Controller for multiple tenants. Microsoft highly recommends migrating to this newly implemented solution and using this carrier and derived trunk model as soon as possible. This allows enhanced monitoring and provisioning for the carrier and his customer tenants.

This Multiple Tenants (Non-Carrier Trunk) example is the same configuration procedure used for a single Direct Routing scenario but has some advanced considerations.

For each tenant, a trunk for the anynode pairing must be created with the domain portion by using the New-CsOnlinePSTNGateway cmdlet. Verify that the given FQDN matches the required domain and subdomains. The voice routings, its policies and all the other Direct Routing related configurations must be set and enabled for each tenant and corresponding user. For anynode, each tenant has to be configured as a Node. The required routing decisions have to be defined through anynode’s routing domain.

Assuming that everything is configured correctly, the example below shows the following routing decisions. A screenshot of this sample is shown on the next page.

As described in the chapter Abstract Processing Overview on page 13, these rule entries will be processed from top to bottom and will follow the first match method. We set the priority up on the defined prefixes of the tenant HQ’s as first rules and place them at the top of the list. Please note that the required dial string manipulations for setting up proper SIP “From:” and “To:” headers for each Node are not shown in detail here.

- Initial all matching numbers starting with prefix +4953638195 from any defined source Node will be forwarded to the configured Tenant ABC (HQ Germany).
- Next, all matching numbers starting with prefix +178185041 from any defined source Node will be forwarded to the configured Tenant DEF (HQ USA).
- All prefixes starting with +1 will be routed to a SIP provider based in the USA.
- All prefixes starting with +49 will be routed to a SIP Provider based in Germany.
- If none of the previous defined rules match, everything else will be forwarded to the PBX Node.
Configuration screenshots of the described example on the previous page:
4.10 Considerations for Media Bypass

Please note that anynode’s default configuration for the Microsoft Teams Direct Routing Node is working very well, at least according to our own experience thus far. That means that anynode is by default enabled for full ICE support and this allows using Microsoft Teams Direct Routing topologies with and without Media Bypass. Generally, there shouldn’t be any configuration changes required for anynode, and once Media Bypass is enabled for your tenant and has been properly configured, the Teams clients will be able to exchange the media traffic via a shorter route to the anynode SBC.

Having said that, before you proceed, please also familiarize yourself with Microsoft Teams Online Call Flows and Plan for media bypass with Direct Routing articles. Here you will find the Teams Online call flow basics, which are recommended and used by Microsoft. Take note of the following general requirements and considerations for enabling Media Bypass:

- Verify that Media Bypass is enabled and available for your tenant. When in doubt, please check with Microsoft about its availability and approval for your tenant.

- Verify that the public IP address or FQDN and the required media port ranges are reachable by the Teams client and routable through your network topology (e.g. in firewalls, gateways, etc.) and with the anynode SBC pairing.

- You must also verify that Media Bypass is also enabled for the anynode SBC pairing. In addition to the used configuration, which is described in chapter Pair the anynode Software SBC to the Tenant on page 9, Media Bypass needs to be enabled. This is done with the optional parameter -MediaBypass $true that can be set via the New-CsOnlinePSTNGateway or Set-CsOnlinePSTNGateway cmdlet (depending on whether this is a newly created or already existing OnlinePSTNGateway).

- If you consider enabling ICE Lite support, please check closely in Appendix A. Lite and Full Implementations of the referring IETF ICE (Interactive Connectivity Establishment) RFC about its advantages and disadvantages. anynode supports Microsoft’s Full ICE implementation, which is also the preferred and supported ICE implementation of the Microsoft Teams clients. This method was recently chosen as anynode’s default for the Microsoft Teams Direct Routing Node.

Please complete reading the whole chapter if you consider enabling ICE Lite.
In order to enable/use ICE Lite (instead of anynode’s default with Full ICE support) please proceed as follows:

- First the detail level for the ICE Protocol settings has to be increased.
- Then you can also see Specify ICE Protocol Properties.
- After enabling this checkbox, the option Use LITE implementation must be enabled.

Please note that the marked screenshot settings only refers to ICE Lite which is not the preferred method.
When ICE Lite is used, you need to keep the following in mind:

- **ICE Lite agents can only offer one (typ host) candidate pair (for RTP and RTCP) in the SDP offer which is part of the SIP INVITE that is signaled to anynode’s Microsoft Teams Direct Routing Node.** The relevant parts of the INVITE would then look similar to the example shown below.
  For comparison: Full ICE agents can offer 2 (or even more) suitable (typ host) candidate pairs.

- **ICE Lite agents don’t perform any connectivity checks or run the state machines, though they need to be able to respond to connectivity checks.**
  For comparison: Full ICE agents will, of course, perform connectivity checks.

```plaintext
INVITE sip:+1234567890@sip.pstnhub.microsoft.com SIP/2.0
... User-Agent: anynode/3.16.x
Via: SIP/2.0/TLS 10.xxx.xxx.xxx:5060;branch=z9hG4bKab7f0476-80f7-4f21-91bc-f30d92776aca
... o=- 1461242293151507626 1 IN IP4 10.xxx.xxx.xxx
... a=ice-lite
... a=ice-ufrag:VYF5ldeo
a=ice-pwd:12ezCISTR+E4xCr3dF8fE90PNa
a=candidate:11 1 UDP 268435711 10.xxx.xxx.xxx 12889 typ host
a=candidate:12 2 UDP 268435710 10.xxx.xxx.xxx 11847 typ host
... 
```

So, when ICE Lite is used, anynode will select the IP address as the (typ host) candidate, which is configured for the Network Controller of the MS Teams DR Node. When this is a public IP address that is reachable from the external network (which is one of the requirements that are listed on page 4) this should not pose any problems. However, there could be policies in place (network security concerns, etc.) that don’t allow the use of a public IP address, but only allow an internal one.
In the latter case, in particular when ICE Lite is used, these further adjustments are required (an example is given in the screenshot below):

- In the Microsoft Teams Direct Routing Node (under Media Negotiation -> Settings -> NAT Traversal) you need to configure a Network Mapping. In particular you need to enter the external Host or IP address (or FQDN) as you can see it in the below screenshots. You may also need to specify UDP and/or TCP Port Mappings (depending on your network requirements).
- In addition you would also need to configure appropriate port forwarding and NAT rules (1:1 NAT) on additional components in your network infrastructure that may reside between the anynode server and Teams DR (e.g. firewalls, gateways, etc.) with its anynode SBC pairing.
4.11 License

Ensure that a license key is available for appropriate functionality. Additional licensing information will be given in the document anynode TechNote (en) - License on demand or our licensing video.
Microsoft's Configure a Session Border Controller for multiple tenants article will give us an example of using a carrier trunk with Direct Routing. Microsoft and anynode partners have management, processing, and configuration optimizations for their customer tenants. The newly implemented logic behind this method is using a single carrier trunk (a carrier tenant created via the CsOnlinePSTNGateway) PowerShell cmdlet and adding derived trunks for their customers.
Those derived trunks and configuration parameters don’t need to be created separately via PowerShell cmdlets as the association is based on the added FQDN's of the carrier tenant. We can reference Microsoft’s article and the description of the Provisioning logic and example. This article will allow us to give a guided configuration example with anynode next.

Please take note that:

- A new domain can only be added by a user with an assigned Global Administrator role. For more details, please check with the Microsoft Docs article About admin roles.

- All newly created domains must be activated by adding at least one user with assigned E1, E3, or E5 license whose credentials match the FQDN portion of the SIP address and the created base domain.

- Domain verifications and updating of the DNS settings process through the Microsoft 365 admin center are not shown or described in detail here. For detailed DNS related information, please check with the Microsoft Docs articles Get help with Office 365 domains and Create DNS records at any DNS hosting provider for Office 365.

Take note that this example uses two CsOnlinePSTNGateway entries in the carrier trunk (anynodesbc.com) for enabling possible failover or load balancing scenarios for the customer tenants. Details will be shown on the next page.
Briefly described domain and FQDN logic and overview of configuration examples:

- **anynodesbc.com** is the default domain of the carrier.
- **customer.anynodesbc.com** is the registered base domain of the carrier tenant, which must be set in the Microsoft 365 admin center.
- **sbc1.customer.anynodesbc.com** is the FQDN used for one of the carrier’s deployed servers using anynode as software SBC. This FQDN is set as OnlinePSTNGateway in the carrier tenant.
- **sbc2.customer.anynodesbc.com** is another FQDN used by the carrier for a second deployed server using anynode as software SBC. This can be used for possible fallback, failover or load balancing scenarios in a Microsoft Teams Carrier Trunk scenario.
- **net4home.de** is the verified default domain used by the customer. **net4home.sbc1.customer.anynodesbc.com** and **net4home.sbc2.customer.anynodesbc.com** are the owned domains for the customer tenant that belong to the carrier tenant.
- **te-systems.com** is the verified default domain used by another customer tenant. **te-systems.sbc1.customer.anynodesbc.com** and **te-systems.sbc2.customer.anynodesbc.com** are the owned domains for the customer tenant that belong to the carrier tenant.
5.1 Microsoft Teams Carrier Tenant

The Microsoft Teams carrier tenant anynodesbc.com uses customer.anynodesbc.com as the base domain. This required base domain (customer.anynodesbc.com) addition and activation process through the Microsoft 365 admin center is not described in detail. You can refer to the Microsoft article to get more information about this topic.

Note: You cannot use the *.onmicrosoft.com tenant for the domain name. There must be a carrier domain like anynodesbc.com.

As mentioned in the listed FQDN logic before, this example uses two carrier trunks, sbc1.customer.anynodesbc.com and sbc2.customer.anynodesbc.com, which are added via the OnlinePSTNGateway PowerShell cmdlet. Their configuration details are shown on the next page.

Both trunks (CsOnlinePSTNGateways) belong to different hosted servers in the carrier environment. Each of them uses anynode as a session border controller. The carrier must ensure that the required DNS records and FQDN’s (domains and subdomains) are valid, match, and are resolvable. The scope of this document does not include such configuration steps. The Microsoft Teams carrier tenant is configured as follows.

The SIP domain details of the carrier tenant via Get-CsOnlineSipDomain PowerShell cmdlet:

```
PS C:\> Get-CsOnlineSipDomain

Name            Status
----            ------
anynodesbc.com  Enabled
customer.anynodesbc.com  Enabled
sbc1.customer.anynodesbc.com  Enabled
sbc2.customer.anynodesbc.com  Enabled
anynodesbc.onmicrosoft.com  Enabled
```

The Microsoft 365 admin center Domains of the carrier tenant (anynodesbc.com):
The **CsOnlinePSTNGateways** of the different servers which use anynode as software SBC in the carrier tenant in detail:

```powershell
C:\> Get-CsOnlinePSTNGateway -identity "sbc1.customer.anynodesbc.com"
Identity : sbc1.customer.anynodesbc.com
InboundTeamsNumberTranslationRules : {}
InboundPstnNumberTranslationRules : {}
OutboundTeamsNumberTranslationRules : {}
OutboundPstnNumberTranslationRules : {}
Fqdn : sbc1.customer.anynodesbc.com
SipSignalingPort : 5069
FailoverTimeSeconds : 10
ForwardCallHistory : True
ForwardPai : False
SendSipOptions : True
MaxConcurrentSessions : 60
Enabled : True
MediaBypass : True
GatewaySiteId :
GatewaySiteLbrEnabled : False
FailoverResponseCodes : 408,503,504
GenerateRingingWhileLocatingUser : True
PidfLoSupported : False
MediaRelayRoutingLocationOverride :
ProxySbc :
BypassMode : None

C:\> Get-CsOnlinePSTNGateway -identity "sbc2.customer.anynodesbc.com"
Identity : sbc2.customer.anynodesbc.com
InboundTeamsNumberTranslationRules : {}
InboundPstnNumberTranslationRules : {}
OutboundTeamsNumberTranslationRules : {}
OutboundPstnNumberTranslationRules : {}
Fqdn : sbc2.customer.anynodesbc.com
SipSignalingPort : 5067
FailoverTimeSeconds : 10
ForwardCallHistory : True
ForwardPai : False
SendSipOptions : True
MaxConcurrentSessions : 60
Enabled : True
MediaBypass : True
GatewaySiteId :
GatewaySiteLbrEnabled : False
FailoverResponseCodes : 408,503,504
GenerateRingingWhileLocatingUser : True
PidfLoSupported : False
MediaRelayRoutingLocationOverride :
ProxySbc :
BypassMode : None
```

We recommend using subdomains like "customer." or "customers." for clearly indicating that this is the carrier trunk base domain used for the derived trunks of the associated customer tenants.
5.2 Microsoft Teams Customer Tenants

The Microsoft Teams carrier trunk model doesn’t require setting up CsOnlinePSTNGateways for the customer tenants. It is only necessary to set the associated domains in the customer tenant. This configuration step must be done before setting up the CsOnlineVoiceRoutes via the PowerShell cmdlet.

Note: The addition and activation process through the Microsoft 365 admin center is not described in detail here. Setting this up also requires appropriate user rights (assigned Global Administration role) for the customer tenant.

The configuration can only be activated by adding one user who is assigned the correct credentials and a SIP address with the FQDN portion that matches the subdomain in the customer tenant. The user also needs an appropriate license. After the successful creation of the subdomain, the license is no longer necessary and available for an active user. Please verify the existence of the domain with the following cmdlet.

In our example, we create two users:

dummy@net4home.sbc1.customer.aynode.de
dummy@net4home.sbc2.customer.aynode.de

The availability of customer tenant domains can be examined by using the Get-CsOnlineSipDomain cmdlet.

```
PS C:> Get-CsOnlineSipDomain

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>net4home.de</td>
<td>Enabled</td>
</tr>
<tr>
<td>net4home.sbc1.customer.aynodesbc.com</td>
<td>Enabled</td>
</tr>
<tr>
<td>net4home.sbc2.customer.aynodesbc.com</td>
<td>Enabled</td>
</tr>
<tr>
<td>net4homegmbh.onmicrosoft.com</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
```
The domains for the customer tenant **net4home.de** are **net4home.sbc1.customer.anynodesbc.com** and **net4home.sbc2.customer.anynodesbc.com**.

**Important:** Review the SBC domain names section of Microsoft Teams Plan Direct Routing documentation. “It might take up to 24 hours to fully provision the domain name after it is added to Domains of your tenant, a user with a new name is created, and a license is assigned to the user”.

---

**Microsoft 365 admin center**

**Domains**

<table>
<thead>
<tr>
<th>Domain name</th>
<th>Status</th>
<th>DNS provider</th>
<th>DNS health</th>
<th>Setup</th>
<th>Identifies</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>net4home.de (Default)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>net4home.sbc1.customer.anynodesbc.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>net4home.sbc2.customer.anynodesbc.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>net4homeglobal.corporate.com</td>
<td></td>
<td>Microsoft</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The **CsOnlineVoiceRoute** sample entries for the customer tenant **net4home.de** are:

PS C:\> set-CsOnlineVoiceRoute -Identity "Germany +49" -OnlinePSTNGatewayList @{add="net4home.sbc1.customer.anynodesbc.com"}
PS C:\> set-CsOnlineVoiceRoute -Identity "Germany +49" -OnlinePSTNGatewayList @{add="net4home.sbc2.customer.anynodesbc.com"}

In our example, this route configuration will route all calls from Teams client with the “+49” prefix to the two configured SBCs in the designated carrier environment. Please change the number pattern to your needs.

The voice routes of the customer tenant **net4home.de** in detail:

PS C:\> Get-CsOnlineVoiceRoute
Identity : Germany +49
Priority : 1
Description : $net4home.de voice route
NumberPattern : ^\+49\((\d{3,20})\)$
OnlinePstnUsages : {anynodesbc}
OnlinePstnGatewayList : {net4home.sbc1.customer.anynodesbc.com, net4home.sbc2.customer.anynodesbc.com}
Name : Germany +49

The additional customer tenant of this example is **te-systems.com** and set up with the domains **te-systems.sbc1.customer.anynodesbc.com** and **te-systems.sbc2.customer.anynodesbc.com**. The **CsOnlineVoiceRoute** definitions are similar to the ones of the other customer tenant and thus not shown in detail.
5.3 Guided anynode Setup

The setup will be created through the anynode wizard. For the carrier trunk scenario, the assistant's Microsoft Teams Direct Routing and a VoIP Provider relationship will be selected. **Add Node** can be alternatively used for creating a new or additional Node for an existing Microsoft Teams Carrier Trunk configuration in anynode. The guided setup through the anynode wizard will be described on the first variant, but both initial setup dialogs are shown on the next screenshot.

Please note that the configuration of **The Voice over IP Provider** Node is not shown in detail as the scope of this guide is on how to set up to the Microsoft Teams carrier trunk. If required, please check with the given Voice over IP Provider Node example on page 23. We proceed with the **Microsoft Teams Direct Routing Carrier Trunk** Node configurations.
In the **Microsoft Teams** dialog, select **Microsoft Teams Direct Routing Carrier Trunk**.

For the **MS Teams Carrier Node** dialog, **Create a new Microsoft Teams Connectivity** is selected as no connectivity is available. For the **Network Controller**, a new one must also be created. Ensure that **reverse DNS Lookup** stays **enabled** for the public interface as this is a requirement for SIP through TLS connections.

If multiple anynode **Network Controllers** share the same network interface on the host, make sure that the port ranges are unique to avoid any port conflicts. The Microsoft Teams Direct Routing Carrier Node is set and uses the default port 5067.
Microsoft Teams with Direct Routing

The **Certificate and Privacy Key** and **Certificate Chain** are imported and used, as shown in the screenshots below and on the next page. Ensure that the certificates include the correct information and all the required FQDN's as SAN's (**Subject Alternative Names**).

The Teams Direct Routing Interface only allows TLS connections from SBC devices with a certificate signed by one of the trusted Certificate Authorities. The currently supported Certification Authorities are available in the Microsoft documentation at:

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc

In this example, the **Subject Alternative Names** include both, the complete FQDN and the one with the wildcard (sbc1.customer.anynodesbc.com and *.sbc1.customer.anynodesbc.com) as shown next:

<table>
<thead>
<tr>
<th>Subject</th>
<th>Subject Alternative Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN=sbc1.customer.anynodesbc.com</td>
<td>*.sbc1.customer.anynodesbc.com (DNS)</td>
</tr>
<tr>
<td>sbc1.customer.anynodesbc.com</td>
<td>(DNS)</td>
</tr>
</tbody>
</table>
The same configuration steps are also necessary for the second SBC with FQDN `sbc2.customer.anynodesbc.com`. 
The configuration of the SBC FQDN is the next step. In this example, `sbc1.customer.anynodesbc.com` is used. The FQDN’s in this dialog are determined from the previously imported certificates. If there are incorrect or missing FQDN’s, go back to the previous assistant configuration and ensure that the correct certificates are used and imported. This **SBC FQDN** is set in the **SIP Transport** configuration dialog of the Node. An example is given in the chapter **SBC FQDN** on page 66.

For the **Tenant FQDN**, only the intended customer part must be set, here `net4home`. Based on this, the complete FQDN `net4home.sbc1.customer.anynodesbc.com` is automatically built.

Please note, this tenant FQDN is set in **Microsoft Teams Tenant** configuration dialog of the customer Node. An example is shown in the chapter **Tenant FQDN** on page 65.
With a new setup, the initial **Routing Domain** will be set after running through anynode’s wizard. So for now, this dialog must be skipped as no routing domain exists. However, for an already present anynode configuration with existing routing domains, you may select the required one.

Next, a default Node name is set, which can be renamed if needed.
Now the **Node Interconnection Assistant** gives an overview of the already performed configuration. Take note that the **Remote SIP Domain** is automatically set to `customer.anynodesbc.com`. If everything is correct, proceed with **Next** to determine the routing behavior for this scenario.

For the routing, the **Use dial string routing** method is used. This ensures that the routing is restricted to a specific dial string. In this example, the routing is set, as shown below.

If everything is set, continue with **Finish** to complete the guided setup in the anynode wizard. Don’t forget to **Commit** afterward to save the newly created configuration.
### 5.3.1 Additional Customer Tenant Nodes

The additional customer tenant nodes are using the same FQDN of the Session Border Controller (SBC FQDN, here `sbc1.customer.anynodesbc.com`) but of course their own verified FQDN part, for this Node and tenant **te-systems**. As the configuration steps through anynode’s assistant are nearly the same as before, they are not completely described.
The vital configuration step for the second customer tenant Node is taking place in the assistant’s **MS Teams Carrier Node** dialog. This additional Node is using the same **SBC FQDN** of the carrier tenant **sbc1.customer.anynodesbc.com**. It is intended to share the configuration of the created **Microsoft Teams Connectivity** object. In this example, the existing **Microsoft Teams net4home** will be selected. This allows the addition and handling of multiple tenants, each with a unique FQDN belonging to the same Microsoft Teams Carrier Trunk very easily.
Microsoft Teams with Direct Routing

In the Select an existing Node to share the Microsoft Teams Connectivity option for this customer tenant Node, both are sharing the same configuration being referenced to the same Microsoft Teams Connectivity object within anynode.

The tooltip information of the Microsoft Teams Connectivity dialog shows which nodes a referenced.

The set Tenant and SBC FQDN for each Node can be reviewed in the Microsoft Teams Tenant and SIP Transport configuration dialog. The details can be reviewed in the screenshots shown in the chapters Tenant FQDN on page 65 and SBC FQDN on page 66.

The Microsoft Teams Connectivity relations of both nodes can be reviewed in the screenshot of the same-named chapter on page 67.

The SIP Domain or the base domain of the carrier tenant, is set in the SIP Node dialog of each customer tenant. The details can be reviewed in the chapter SIP Domain on page 68.
5.3.2 Tenant FQDN

The customer tenant FQDN’s set through the anynode wizard for each Node can be reviewed in the Microsoft Teams Tenant dialog. In this configuration example, net4home.sbc1.customer.anynodesbc.com and te-systems.sbc1.customer.anynodesbc.com are shown below.

![Microsoft Teams with Direct Routing Diagram](image-url)
5.3.3 SBC FQDN

The carrier-related SBC FQDN that was set through the anynode wizard can be reviewed in the SIP Transport dialog of the Node. In this configuration example `sbc1.customer.anynodesbc.com`.
5.3.4 Microsoft Teams Connectivity

The details of the Microsoft Teams Connectivity dialogs of both customer tenant nodes is shown below. Both are referenced to the Microsoft Teams Connectivity SIP Node object.
5.3.5 SIP Domain

The carrier-related **SIP Domain** that has been set can be reviewed in the **SIP Node** dialog. The screenshot below shows the choices used for this configuration example. Both are set to the **customer.anynodesbc.com** FQDN.
5.3.6 Routing Domains

We recommend using multiple routing domains if each customer tenant Node belongs to a single provider Node with different user data and unique credentials. You can see an example of this scenario on the following screenshots.
E911 Dynamic Emergency Calls with Microsoft Teams

Dynamic emergency calling for Microsoft Calling Plans, and Phone System Direct Routing provides the capability to configure and route emergency calls and notify security personnel based on the current location of the Teams client. In many companies, emergency calling is not a top priority of their Microsoft Teams “to-do” list. The increasing number of remote, distributed, and mobile workforces make moving your on-prem equipment to a cloud-based platform like Teams challenging. Phones are no longer dedicated to a specific location and user moving around in different buildings. Microsoft Teams offers a concept to add civic addresses to different types of endpoints in your network infrastructure. This location information can be transferred to anynode to transfer your call to your next PSAP. In case your SIP trunk is already busy with other traffic, anynode will drop a call and clear the path for your emergency concern.

anynode is officially certified for E911 emergency calling with Microsoft Teams and validated with the following E911 SIP carriers in the United States:

- RedSky
- Bandwidth
- Intrado

For details about managing emergency calling in Microsoft Teams, please check with the appropriate Microsoft docs.
6.1 Example: anynode with an E911 Provider

Please note that this emergency call example is independent of the other configurations shown in this TechNote. NOTE: Microsoft recommends that Direct Routing customers in the United States should coordinate with their ERSP for a test service!

6.1.1 Routing Domain

The Routing Domain entry for this **E911 Provider** configuration sample is described next. The filter rule has to match the defined emergency call prefix of the Microsoft Teams Direct Routing tenant source node which must be forwarded to the referring destination node of the Service Provider. The matching prefix in this example is **+911**. You may have to use 911, or initially using a test number of your E911 service provider, for example +933, or even others digits depending on the provider requirements. The filter rule entry is named **To E911 VoIP Provider** and referenced to a **Routing Forward Profile**. This profile contains specific **Telephony Forwarding** values that determine which information has to be forwarded from the calling entity to the called entity and vice versa. The **Routing Forward Profile** chapter from page 72 will describe its settings.

**Important**: As the filter rules of anynode will be processed from top to bottom, using the first match method, the emergency entry must always be moved to the top of the filter list. This ensures that no other filter rule will match before and thus avoid matching conflicts.

![Routing Domain Diagram](image-url)
6.1.2 Routing Forward Profile

This **Routing Forward Profile** shows the important settings of the referenced To E911 VoIP Provider Routing Domain entry as described in the previous chapter from page 71. **Important:** Value Specify whether the SIP geolocation information should be forwarded must be enabled. This option is located in the **Signaling Forwarding from Calling Entity to Called Entity** section of the **Telephony Forwarding** configuration dialog, close to the bottom of the list. This value must be enabled for the referenced Routing Forward profile to handle the provided .xml body payload from the Microsoft Teams emergency call with the location details of the user through the anynode SBC towards the E911 service provider upon his requirements. An example is shown on the screenshot below.

The chapter **Plan and Configure Dynamic Emergency Calling for Microsoft Teams Direct Routing** starting on page 75 will give a brief overview on the Microsoft Teams Direct Routing related configuration. The chapter **Test and Check Geolocation and E911 Related Emergency Call Headers** from page 77 gives some information how the check about the .xml body payload.
6.1.3 SIP User Agent - RFC 6442

Option Specify whether RFC 6442 (Geolocation forwarding) is enabled is set by default. If required, this option can be reviewed in the SIP User Agent configuration dialog of the participating nodes as shown in the screenshot below.
6.1.4 SIP User Agent - Processing SIP Geolocation ELIN URI

You may have to pass the SIP Geolocation ELIN URI of the Microsoft Teams environment in specific SIP headers towards the provider. The example below shows that the provided SIP Geolocation ELIN URI of the Teams environment should be handed over as P-Asserted-Identity header.
6.2 Plan and Configure Dynamic Emergency Calling for Microsoft Teams Direct Routing

The Microsoft Teams Direct Routing and E911 Provider related configurations are out of scope of this document and thus not shown in detail here. The configuration needs enhanced knowledge and awareness about the requirements for emergency calling from these parties. For configuration details and examples, please check with the Plan and configure dynamic emergency calling of the Microsoft Docs, as well as with the ones of the certified E911 service provider. A brief overview about the Microsoft Teams related configurations is given next.

- Provide the public IP addresses of the Teams clients and users which has to match the Trusted IP's in the tenant (corporate network, public NAT IP) via the Teams admin center or PowerShell New-CsTenantTrustedIPAddress cmdlet.

- Setup a Network site (CsTenantNetworkSite) with its appropriate configuration: Network Region and Location Information Service (LIS) relations of the tenant, Subnets (CsOnlineLisSubnet), WAPs (CsOnlineLisWirelessAccessPoint), Ports (CsOnlineLisPort), Switches (CsOnlineLisSwitch).

- Define the Civic Address through the Emergency addresses of the Teams admin center, or via PowerShell cmdlet CsOnlineLisCivicAddress with its parameters including Elin and Location. Confirm the emergency location with Get-CsOnlineLisLocation.

- Ensure that the –PidfloSupported $true parameter is set for anynode’s CsOnlinePSTNGateway. This enables the PIDF-LO support, the .xml body payload with the location details of the Teams user.

- Define the emergency and call routing policies (CsTeamsEmergencyCallingPolicy and CsTeamsEmergencyCallRoutingPolicy) which must be applied to the Teams users that needs to be enabled for E911 via Grant-CsTeamsEmergencyCallRoutingPolicy -Identity PowerShell cmdlet, or via the Teams admin center (Voice -> Emergency policies).

- Ensure that the Enhanced emergency services option is enabled (Teams admin center -> Emergency services, or PowerShell cmdlet CsTeamsEmergencyCallRoutingPolicy –AllowEnhancedEmergencyServices $true).
**Important:** If the Microsoft Teams Direct Routing and client related configurations are correct, the Teams clients will clearly display the call with *Emergency call in progress*. An example is shown on the screenshot below. If this is not the case, please check with your Teams configurations. By all means it must be ensured that all required emergency call address headers will be correctly provided towards anynode and passed to the connected E911 service provider. Please check with the chapter *Test and Check Geolocation and E911 Related Emergency Call Headers* from page 77 for more details.
6.3 Test and Check Geolocation and E911 Related Emergency Call Headers

Before you start placing any ‘real’ emergency calls, the configurations must be extensively tested!

**IMPORTANT:** Please take note of the Microsoft Docs [Test emergency calling](#) chapter. Check and coordinate the E911 test with your ERSP (Emergency Routing Service Provider). Some service providers offers some predefined test emergency numbers, like +933 / 933 in the United States.

Please check with the geolocation and E911 related emergency call headers. Ensure that you are aware about the E911 Provider requirements, and that the provided emergency call headers of the Microsoft Teams Direct Routing environment with its Teams clients will be properly processed from anynode. Verify with the **inbound** SIP notification and the emergency related headers of the Teams environment and clients as well as with the processed **outbound** SIP headers towards the E911 provider with an anynode trace. You must identify incorrect configurations and missing payload information. Check with the ERSP if everything is delivered as expected! An example of an anynode trace with an inbound emergency call is shown next. Please note that this screenshot is shown as a fictitious sample of a test environment using a test bot number and thus might not include all relevant information.
Local Media Optimization with anynode and Microsoft Teams

Local Media Optimization is a new feature within Direct Routing which enables you to keep media local to the network. For instance, a user calling another user within the same organization would keep the call locally on the company’s network.

With Local Media Optimization, Microsoft Teams and anynode enables the optimal RTP media flow for in-house hosted SBC’s with local connections to providers or PBX around the world.

For details please check with the Microsoft Docs articles Local Media Optimization for Direct Routing and Configure Local Media Optimization for Direct Routing.
You can enable this feature in the anynode frontend and on the corresponding Microsoft Teams side. anynode and the Teams server can then distinguish between Teams clients that are on the external public network and Teams clients that are on the internal company network. There are at least two practical applications:

**Option 1: anynode is used as the only SBC in the company network**

anynode is used as the only SBC in the company network and has an internal and an external network card. If an employee within the company network wants to make a call to the PSTN via the Teams client, Teams recognizes that the Teams client is in the internal company network and negotiates with anynode that the RTP media data is exchanged with the Teams client via the internal network card / IP address. If a mobile employee now wants to use his external Teams client for a call to the PSTN outside of the company network, the external network card / IP address is used for the RTP voice data.
Microsoft Teams with Direct Routing

Option 2: anynode is used as Proxy SBC with a Site SBC in the company network

In this scenario, all calls go to anynode, which is configured as a Proxy SBC. They are then routed to a local anynode as a Site SBC. Configured this way, anynode as Proxy SBC provides access to the Teams server for other Site SBC's in the company network.

An internal and external IP address is also used here. A practical application is to use a single Microsoft Teams Direct Routing connection from several geographically separate locations in a company and the RTP data streams remain local in the respective locations, as long as the Teams client is located in the respective location.

Option 2 briefly described logic: anynode is used as Proxy SBC with a Site SBC in the company network

- **anynodesbc.com** is the default domain and the registered base domain of the tenant set in the Microsoft 365 admin center.

- **sbc1.anynodesbc.com** is the FQDN used on the Proxy SBC (located in Europe/Germany). This FQDN is set in the Office365 Phone System, it must be correctly resolvable through a public DNS carrier with a public IP address.

- **sbc2.anynodesbc.com** is the FQDN used by anynode's Site SBC (located in the USA). This FQDN doesn’t require a resolvable public DNS carrier entry with a public IP address, it just must be reachable within the local network. Please make sure that the FQDN of the Site SBC is included in the configured certificate for the Teams connection.

Each anynode SBC site is bound to a local SIP provider. The SIP provider related configurations are not shown in details.
7.1 Microsoft Teams Tenant with Local Media Optimization

In this example, the **CsOnlinePSTNGateway** of anynode's Proxy SBC is set to the FQDN `sbc1.anynodesbc.com`. Ensure that the **MediaBypass** parameter is set to `true` and the **BypassMode** is enabled in order to support **Local Media Optimization**.

```powershell
PS C:\> Get-CsOnlinePSTNGateway -Identity sbc1.anynodesbc.com

Identity : sbc1.anynodesbc.com
InboundTeamsNumberTranslationRules : {}
InboundPstnNumberTranslationRules : {}
OutboundTeamsNumberTranslationRules : {}
OutboundPstnNumberTranslationRules : {}
Pfgn : sbc1.anynodesbc.com
SipSignalingPort : 5069
FailoverTimeSeconds : 10
ForwardCallHistory : False
ForwardPai : False
SendSipOptions : True
MaxConcurrentSessions : 100
Enabled : True
MediaBypass : True
GatewaySiteId : Intern
GatewaySiteLbrEnabled : False
FailoverResponseCodes : 408,503,504
GenerateRingingWhileLocatingUser : True
PidfLoSupported : False
MediaRelayRoutingLocationOverride : ProxySbc
BypassMode : Always
```

The **CsOnlinePSTNGateway** of anynode's Site SBC here is set to FQDN `sbc2.anynodesbc.com`. For the Site SBC's the **MediaBypass** parameter must be also set to **true** and the **BypassMode** parameter must be set to **Always** or **OnlyForLocalUsers** for enabling **Local Media Optimization** support. The **ProxySbc** parameter must be set to the Proxy SBC FQDN, here it is set to `sbc1.anynodesbc.com`.

```powershell
PS C:\> Get-CsOnlinePSTNGateway -Identity sbc2.anynodesbc.com

Identity : sbc2.anynodesbc.com
InboundTeamsNumberTranslationRules : {}
InboundPstnNumberTranslationRules : {}
OutboundTeamsNumberTranslationRules : {}
OutboundPstnNumberTranslationRules : {}
Pfgn : sbc2.anynodesbc.com
SipSignalingPort : 5069
FailoverTimeSeconds : 10
ForwardCallHistory : False
ForwardPai : False
SendSipOptions : True
MaxConcurrentSessions : 100
Enabled : True
MediaBypass : True
GatewaySiteId : LAB
GatewaySiteLbrEnabled : False
FailoverResponseCodes : 408,503,504
GenerateRingingWhileLocatingUser : True
PidfLoSupported : False
MediaRelayRoutingLocationOverride : ProxySbc
BypassMode : Always
```
The **CsTenantTrustedIPAddress** for managing the external trusted IP addresses for the tenant in this setup is used as follows. Make sure all the external IPs of each site where Teams users are enabled and support Local Media Optimization.

```powershell
PS C:> Get-CsTenantTrustedIPAddress
Identity : 62.76.24.86
MaskBits : 32
Description : IPAddress : 62.76.24.86
Identity : 62.76.24.74
MaskBits : 32
Description : IPAddress : 62.76.24.74
```

The **CsTenantNetworkRegion** cmdlet is used as follows:

```powershell
PS C:\> Get-CsTenantNetworkRegion
RunspaceId : dab38bae-bf25-47c3-b080-3f58079bd51f
Identity : anynodesbc
NetworkRegionID : anynodesbc
Description : NetworkRegionID : anynodesbc.com Region
CentralSite : anynodesbc
RunspaceId : dab38bae-bf25-47c3-b080-3f58079bd51f
Identity : anynodesbcWLAN
NetworkRegionID : anynodesbcWLAN
Description : CentralSite : anynodesbcWLAN
```

Ensure that each network site is associated with the correct network region. The **CsTenantNetworkSite** cmdlet used in this example:

```powershell
PS C:\> Get-CsTenantNetworkSite
RunspaceId : dab38bae-bf25-47c3-b080-3f58079bd51f
Identity : WAN
NetworkSiteID : WAN
Description : NetworkRegionID : anynodesbc
LocationPolicy :
EnableLocationBasedRouting : False
OnlineVoiceRoutingPolicy : SiteAddress :
EmergencyCallRoutingPolicy :
EmergencyCallingPolicy :
RunspaceId : dab38bae-bf25-47c3-b080-3f58079bd51f
Identity : LAB
NetworkSiteID : LAB
Description :
NetworkRegionID : anynodesbc
LocationPolicy :
EnableLocationBasedRouting : False
OnlineVoiceRoutingPolicy : SiteAddress :
EmergencyCallRoutingPolicy :
EmergencyCallingPolicy :
RunspaceId : dab38bae-bf25-47c3-b080-3f58079bd51f
Identity : Internal
NetworkSiteID : Internal
Description :
NetworkRegionID : anynodesbc
LocationPolicy :
EnableLocationBasedRouting : False
OnlineVoiceRoutingPolicy :
SiteAddress :
EmergencyCallRoutingPolicy :
EmergencyCallingPolicy :
```
The **CsTenantNetworkSubnet** is used as shown next. Note that each network subnet can only be associated with one site.

```
PS C:\> Get-CsTenantNetworkSubnet
Identity : 172.6.3.0
Description : 
NetworkSiteID : WAN
MaskBits : 24
SubnetID : 172.6.3.0

Identity : 172.8.0.0
Description : 
NetworkSiteID : LAB
MaskBits : 16
SubnetID : 172.8.0.0

Identity : 172.6.0.0
Description : 
NetworkSiteID : Internal
MaskBits : 23
SubnetID : 172.6.0.0
```

The **CsOnlineVoiceRoute** sample entries for this Proxy (sbc1.anynodesbc.com) and Site SBC (sbc2.anynodesbc.com) environment are:

```
C:\> Get-CsOnlineVoiceRoute
Identity : Germany
Priority : 1
Description : ^\+49\(\d\{3,20\}\)$
OnlinePstnUsages : {Germany}
OnlinePstnGatewayList : {sbc1.anynodesbc.com}
Name : Germany

Identity : USA
Priority : 2
Description : ^\+1\(\d\{3,20\}\)$
OnlinePstnUsages : {USA}
OnlinePstnGatewayList : {sbc2.anynodesbc.com}
Name : USA
```
7.2 Guided anynode Setup for Local Media Optimization

The complete setup will be created from scratch through the anynode wizard. Please note that given examples are independent of the others shown in this document.

In this example, the assistant’s Microsoft Teams Direct Routing and a VoIP Provider relationship will be selected. Add Node can be alternatively used for creating a new or additional nodes for an existing Microsoft Teams configuration in anynode.

The guided setup through the anynode wizard will be described in the first variant, but both initial setup dialogs are shown on the next screenshot.

Please note that the configuration of the Voice over IP Provider nodes for the Proxy and Site SBC are not shown in detail. The scope of this chapter is set to Microsoft Teams with local media optimization. If required, please check with the given Voice over IP Provider Node example on page 23. We proceed with the Microsoft Teams Direct Routing configurations.
In the Microsoft Teams dialog, select Microsoft Teams Direct Routing (Local Media Optimization) for the Proxy SBC location of the tenant.

For the Network Controller and Internal Network Controller dialog the corresponding public and internal network interfaces must be selected. Ensure that reverse DNS Lookup stays enabled for the public interface as this is a requirement for SIP through TLS connections.
If multiple anynode **Network Controllers** share the same network interface on the host, make sure that the port ranges are unique to avoid any port conflicts. The Microsoft Teams Direct Routing Node is set and uses port 5067.
The Certificate and Privacy Key and Certificate Chain are imported and used as shown in the screenshots below. Ensure that the certificates include the correct information and all the required FQDN's as SAN's (Subject Alternative Names), in this example sbc1.anynodesbc.com.
The **SBC FQDN** must be set. In this example `sbc1.anynodesbc.com` is used. The FQDN's in this dialog are determined from the previously imported certificates. If there are incorrect or missing FQDN's, go back to the previous assistant configuration and ensure that the correct certificates are used and imported. This **SBC FQDN** is set in the **SIP Transport** configuration dialog of the Node.

An example is given in the chapter **SBC FQDN** on page 66.

With a new setup, the initial **Routing Domain** will be set after running through anynode’s wizard. For now, this dialog must be skipped as no routing domain exists. However, for an already present anynode configuration with existing routing domains, you may select the required one now.
Next, a default Node name is set which is here renamed to Teams anynodesbc.com.

Now the Node Interconnection Assistant gives an overview of the already performed configuration. Take note that the Remote SIP Domain is automatically set to anynodesbc.com.
Next, the referring SIP provider Node of the anynode Proxy SBC site will be configured. As mentioned before this is not shown in detail, thus the next screenshot gives just an overview.

If everything is correct, proceed with **Next** to determine the routing behavior for this scenario.
The configuration overview of anynode’s Proxy SBC site is shown below. The next configuration step is setting up the Site SBC Node which will be described in the chapter Setting up the Site SBC Node for the anynode Proxy SBC starting on page 92.
7.2.1  Setting up the Site SBC Node for the anynode Proxy SBC

The next step for the anynode Proxy SBC configuration is setting up the Node for the Site SBC. The additional Node can be added via Add Node.

Again the Microsoft Teams entry must be selected.
In the Microsoft Teams dialog, select Microsoft Teams Direct Routing with Local Media Optimization Site SBC as Node type.

For the network controller, select the internal interface that is used for the interaction between the anynode Proxy and Site SBC locations.
Next, set the required local ports, the remote SIP Domain or IP address of the anynode Site SBC (here 172.6.0.153 with port 5074) and the network peer whitelist.
No incoming and outgoing dial string manipulations are required in this example. Regardless of this configuration, the chapter Example: Dial String Manipulations starting on page 39 gives a manipulation example.

The Routing Domain is automatically set. The Node name is here renamed to anynode Site SBC.
7.2.1.1 Set the Site SBC FQDN for anynode’s Proxy SBC Node

As only anynode’s Proxy SBC Node interacts directly with the Microsoft Teams Direct Routing trunk the corresponding Site SBC FQDN must now being set. This has to be added within Microsoft Teams Tenant configuration dialog as described next.

Enable Proxy SBC operation and push the Add button.

Now add the required entry, in this example here FQDN `sbc2.anynodesbc.com` with the anynode Site SBC Node.
The FQDN of the Site SBC is now set.
7.2.2 anynode Site SBC Configuration

The Site SBC, the anynode SBC of the tenant located in the USA, is configured as described next. As the Site SBC is also connected to a local SIP provider, the assistant’s Microsoft Teams Direct Routing and a VoIP Provider relationship will be selected again.

The Microsoft Teams Node defaults are set and its details must be configured.
Microsoft Teams with Direct Routing

For the Site SBC location the Proxy SBC Node has to be created. For this option Microsoft Teams Direct Routing with Local Media Optimization Proxy SBC must be selected as Node type.

Select the corresponding internal network interface that is required for the Proxy SBC interaction.
Next, set the required local ports, the remote SIP Domain or IP address of the anynode Proxy SBC (here 172.8.0.94 with port 5064) and the network peer whitelist.
No incoming and outgoing dial string manipulations are required in this example. Regardless of this configuration, the chapter Example: Dial String Manipulations starting on page 39 gives a manipulation example.

The initial Routing Domain will be set after running through anynode’s wizard in a new setup. The Node name is here renamed to Proxy SBC Germany.
Now the **Node Interconnection Assistant** gives an overview of the completed configuration. Proceed with **Next** to configure the SIP provider Node and the **Routing** decisions for the selected VoIP scenario.

Please note again that the provider related configuration steps are not shown in detail. The next screenshot only shows an overview.
For the routing, the recommended **Use dial string routing** method is used. This ensures that the routing is restricted to a specific dial string. In this example the routing is set as shown below. If everything is set continue with **Finish** to complete the guided setup in the anynode wizard. Don't forget to **Commit** afterwards to save the newly created configuration.
The created routing domain entries with their filter and profile relations for the anynode's Site SBC of this example are shown next:
Appendix

8.1 Test Call

Assuming that Microsoft’s Teams or Phone Mail System is working properly and anynode’s Node states are fine, the scenario can be tested with an external public station or if set with an internal station that calls a Microsoft Teams client or extension through anynode and vice versa.

Review the call flow and routing between the nodes and check that numbering is handled as expected.

In anynode, you can review the active call session and the call history via the Monitor Mode of anynode’s frontend. An Active Sessions or Call History example will be given in the next sections. You can review the SIP flow or more in-depth analysis by using anynode’s Trace Analyzer. Some brief information about Tracing is given in the chapter starting on page 107. The Trace Analyzer chapter starting on page 108 gives some information and call flow examples.

8.2 Active Sessions

Active Sessions can be obtained via anynode’s frontend Dashboard in the Monitor Mode. Move the mouse pointer over the relevant entry which will display more session details.
8.3 Call History

The Call History can be reviewed via anynode’s frontend Dashboard in the Monitor Mode. As for the active sessions, moving the mouse pointer over the relevant entry will display more session details. A double-click on the call history entry will open a new window with several session details.
8.4 Tracing

The anynode Trace Analyzer is used for in-depth analyzing and support requests. To do so, the trace can be activated, deactivated and downloaded within anynode’s frontend Tracing dialog. As soon as activated, a notification will be displayed in the frontend’s upper right corner. The trace file can be downloaded and opened or stored with the file name extension .xztrace. A trace file and captured call flow example will be given in the chapter Trace Analyzer starting on page 108.

Please note, besides capturing signaling and media details the created trace also includes the anynode configuration. Thus, it is not necessary to export the anynode configuration or supply support with any screenshots of the configuration. For support requests, just provide a trace file as described in the next chapter Trace Analyzer starting on page 108.

If anynode's frontend is installed and opened on the same server where all the anynode services are running, the Live Trace option, that is not explained in this document, can be used. However, it has to be ensured that the Trace Analyzer executable is installed where the trace file will be opened and reviewed.
8.5 Trace Analyzer

The anynode Trace Analyzer is a powerful tool for analyzing and debugging. Based on this document's configurations, the next screenshot gives an example of the test mentioned in the chapter Test Call starting on page 105. Besides the captured session overview, an excerpt of its media and audio flow as well as the initial SIP invite is shown.

If the numbering format is not accurate, you may have to create some additional outgoing dial string manipulations in the associated SIP Node. For a more in-depth analysis the streams could be analyzed, but this is beyond the scope of this document and not shown here. More information will be given in the Trace Analyzer and Live trace videos which are available on our YouTube channel.
8.6 Trial Version

Just follow the URL https://www.anynode.de/download/ to request an anynode trial via the website’s download section.
8.7 Hosted in Microsoft Azure

anynode is also available in the Microsoft Azure cloud. Please check with our YouTube video for details.
8.8 anynode Installation

For **Linux**, please check with our **repository server**.

For **Windows**, request a trial as described in chapter **Trial Version** on page 109 and/or download the setup from our **Community**. Install the anynode executable on the appropriate server. Verify that the user account has administrative rights and permissions to do so. If necessary use the **Options** button for changing the default listening port 8088 of anynode’s web frontend. Read and agree with the license terms and conditions and start the installation process by pushing the **Install** button. On success, launch the anynode frontend directly or close the setup.

Before accessing anynode’s web frontend, you may want to check the status of its running services.

As installation default anynode’s web frontend is reachable on the local host (http://localhost:8088/ or http://127.0.0.1:8088/ unless the port was changed through the setup options.)
8.9 Information, License and Support Requests

Visit our website to keep up with our products, contact information, video guides and tutorials and documentations. Take a look in the anynode academy for training and workshop related information. Contact our sales team for any license related questions or general questions about our products. For support requests, contact our support team with a short and precise description of the issue. Attach a trace showing the described scenario. If not restricted through the trace options, the generated trace file also includes the anynode configuration. The tracing will be described in the corresponding chapter on page 107. For new e-mail requests a ticket will opened and our ticket system automatically generates a reply with a ticket number which is used for reference purposes. Please do always refer to that ticket number if doing any e-mail or phone requests.
Exclusion of Liability

Copyright © 2021 TE-SYSTEMS GmbH

All rights reserved

This document, in part or in its entirety, may not be reproduced in any form without the prior consent of TE-SYSTEMS GmbH.
The information contained in this document was correct at the time of writing. TE-SYSTEMS GmbH reserves the right to make any alterations without prior notice.
The utmost care was applied during the compilation of texts and images, as well as during the creation of the software. Nevertheless, no responsibility can be taken for the content being accurate, up to date or complete, nor for the efficient or error-free operation of the software for a particular purpose. Therefore, TE-SYSTEMS GmbH cannot be held liable for any damages resulting directly or indirectly from the use of this document.

Trademarks

All names of products or services used are trademarks or registered trademarks (also without specified indication) of the respective private or legal persons and are therefore subject to legal regulations.

Third Party Disclaimer and Limitations

"Web Toolkit", developed by Google (http://code.google.com/webtoolkit/).
"Smart GWT", developed by Isomorphic Software, Inc. (http://www.smartclient.com/).
"Jetty", developed by Mort Bay Consulting Pty Ltd (http://mortbay.com/).
"Apache Commons IO", developed by the Apache Software Foundation (http://www.apache.org/).
"Guava Libraries", developed by Google (http://code.google.com/p/guava-libraries/).
"LDAP SDK", developed by Unbound ID (https://www.unboundid.com/products/ldap-sdk/).
"Freemarker", developed at freemarker.org (http://freemarker.org/).
"jsoup", developed by Jonathan Hedley (http://jsoup.org/).
"OpenSSL", developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/), written by Eric Young (eay@cryptsoft.com) and written by Tim Hudson (tjh@cryptsoft.com). [Windows only]
"Opus codec", developed by the Xiph Foundation (http://www.opus-codec.org/license/).
"SQLite", developed at sqlite.org (https://sqlite.org/).
"Java Runtime", developed by Oracle Corporation (JRE License Terms). [Windows only]
"SilK codec", developed by Skype Limited (https://www.skype.com/)

anynode-Frontend

This product includes software developed by Google (http://code.google.com/webtoolkit/)
This product includes software developed by Isomorphic Software, Inc. (http://www.smartclient.com/)
This product includes software developed by Mort Bay Consulting Pty Ltd (http://mortbay.com/)
This product includes software (JNA) developed at github.com (https://github.com/twall/jna)
This product includes software developed by the Apache Software Foundation (http://www.apache.org/)