

ALL IN COMMUNICATION

Anforderungen an die Infrastruktur am Kundenstandort
V 2.5



Inhalt

ALL IN COMMUNICATION	1
Inhalt.....	2
Allgemeines	3
Anbindungsvarianten	3
Variante A: Getrennte AIC Infrastruktur mit eigenem LAN Switch.....	3
Variante B: Getrennte AIC Infrastruktur mittels VLAN.....	4
Variante C: Gemeinsame AIC Infrastruktur	5
Sonderfall PC hinter VoIP Telefon	7
Zusätzliche Anforderungen an das Netzwerk.....	7
Firewall Regeln	7
Verwendete IP Adressen.....	8
Switched LAN Umgebung (< 30 bis 50 Arbeitsplätze)	8
LAN Umgebung (> 50 Arbeitsplätze)	9
VoIP VLAN.....	9
VoIP VLAN Zusatzanforderungen	9
Quality of Service (QoS) Funktionen im LAN Switch.....	10
Einstellung bei Verwendung eines Faxgerätes	10
Anhang	11
Plattform Kommunikation.....	11
Softclients DesktopControl und DesktopOperator.....	11
Torsprechanlagen, Türöffner und automatische Schrankenanlagen	12
VPN Verbindungen im Kunden LAN	12
DHCP Optionen für Telefone außerhalb des AIC VoIP LAN.....	12
DHCP Optionen für Cisco/Panasonic/Snom	13
DHCP Optionen für Unify OpenStage Telefone.....	13



Allgemeines

Vor dem Installationstermin der All In Communication Hardware (Telefone, Analog-Adapter, Fax-Adapter) ist zur Sicherstellung der einwandfreien Funktion und der reibungslosen Inbetriebnahme kundenseitig die LAN-Infrastruktur entsprechend vorzubereiten bzw. anzupassen.

Die folgende Beschreibung richtet sich an den Netzwerkverantwortlichen des Kunden.

Anbindungsvarianten

Um einen störungsfreien Betrieb des VoIP Dienstes zu gewährleisten, wird ein eigener VoIP Anschluss bereitgestellt. Der vor Ort installierte AIC Router auf diesem Anschluss gilt hier als Übergabepunkt der Netzwerkkommunikation des AIC Dienstes in das Kundennetz.

An diesen Anschluss können die VoIP Endgeräte in verschiedenen Varianten angeschlossen werden.

Variante A: Getrennte AIC Infrastruktur mit eigenem LAN Switch

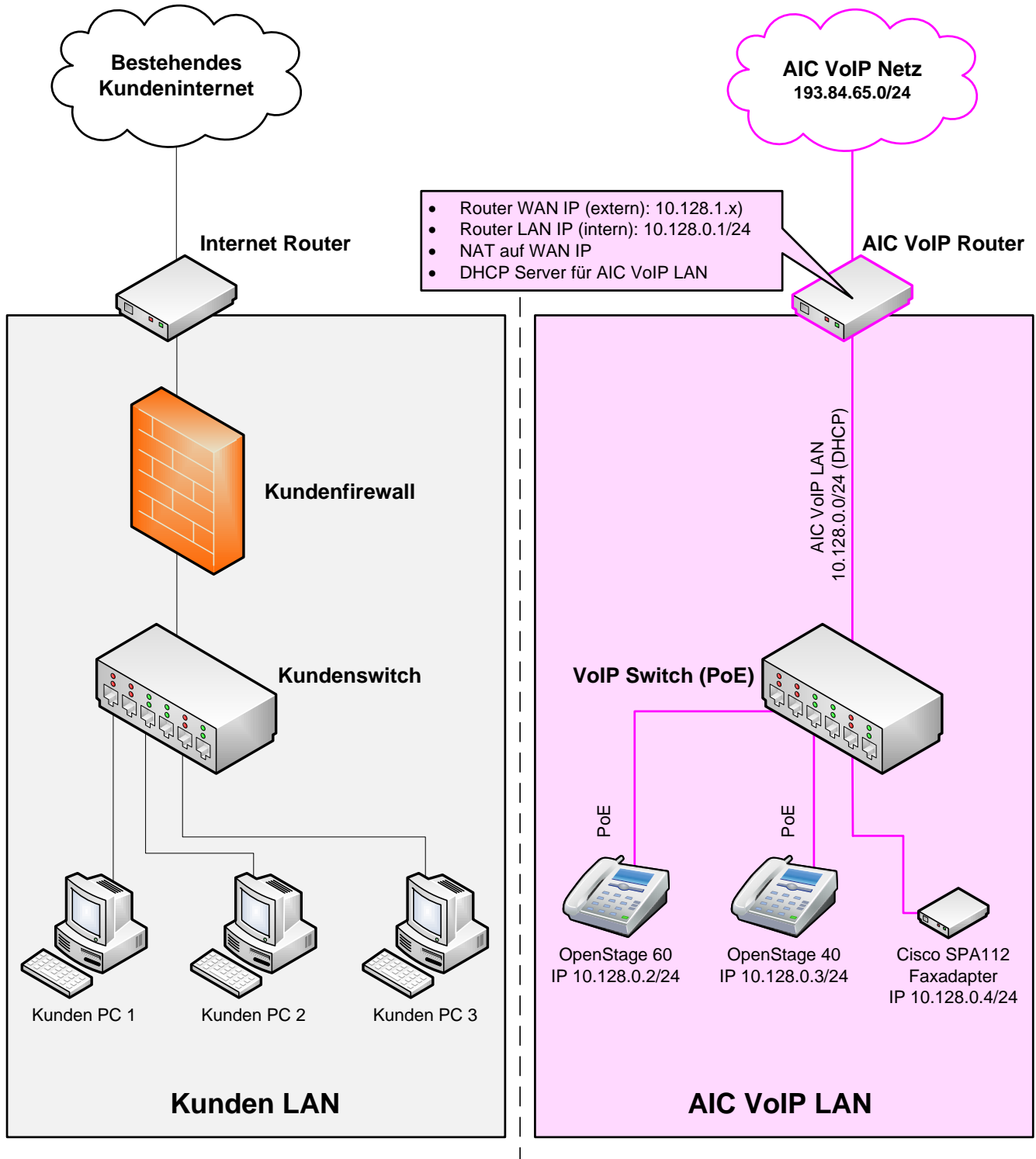
In dieser einfachen und robusten Variante wird die bestehende Netzwerk-Infrastruktur des Kunden nicht verändert. Die Installation der Telefone läuft parallel zur IT Umgebung des Kunden auf einer eigenen Verkabelung. Wechselwirkungen sind somit ausgeschlossen.

Die Verkabelung und der LAN Switch müssen vom Kunden bereitgestellt werden.

Der Vorteil dieser Variante ist deren Einfachheit

Hinweis: Softclient mit VoIP Funktion (Desktop Communicator, Desktop Operator) können hier nicht eingesetzt werden.





Variante A: Getrennte AIC Infrastruktur mit VoIP Switch

Variante B: Getrennte AIC Infrastruktur mittels VLAN

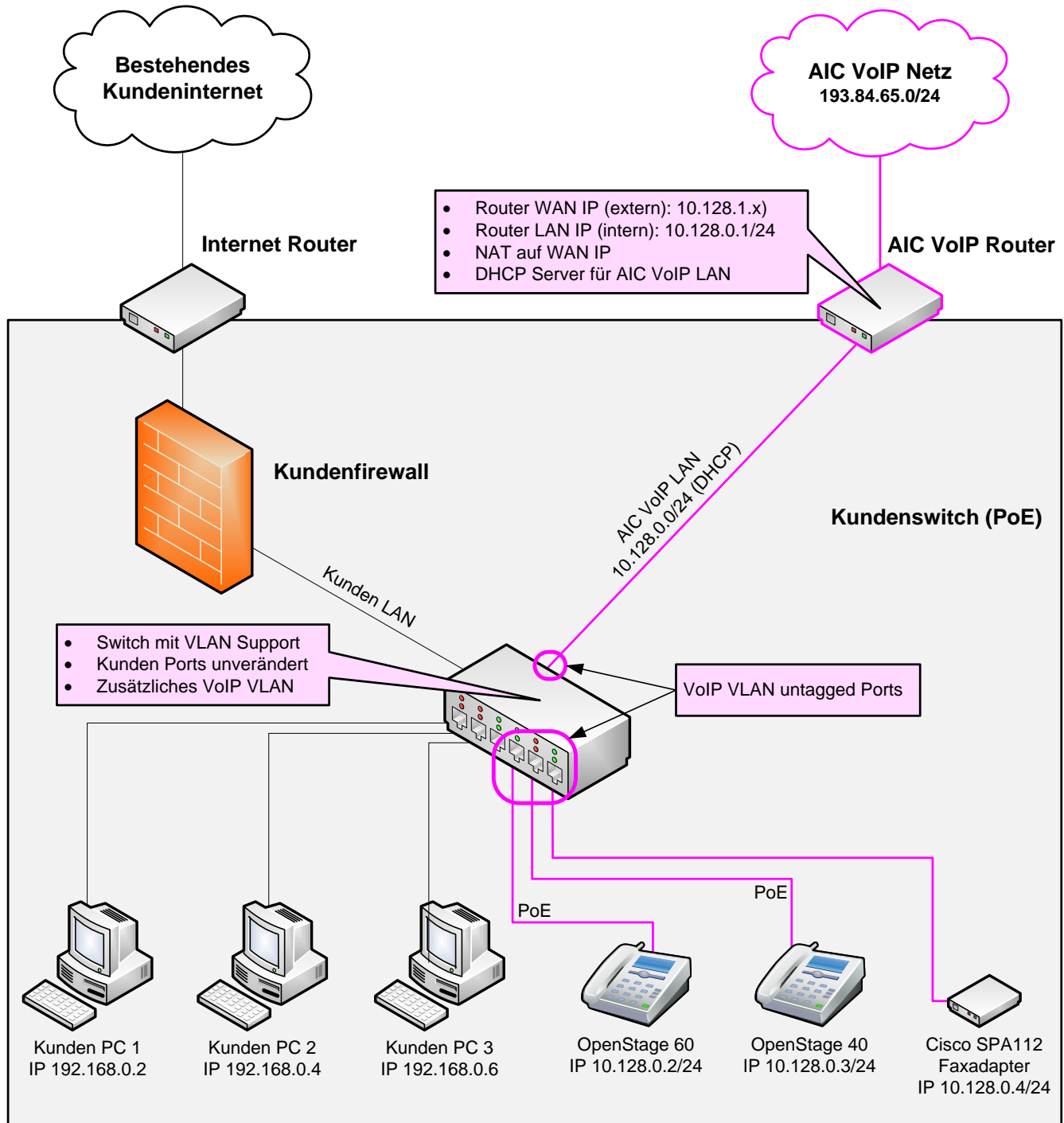
In dieser Variante wird anstelle des eignen LAN Switches aus Variante A ein getrenntes, unabhängiges, nicht anderweitig verwendetes Virtual-LAN (VLAN) am VLAN fähigen, bestehenden Kunden LAN Switch verwendet. Es gilt zu beachten, dass es keine IP Verbindung zwischen dem VoIP VLAN und dem Kunden LAN gibt und geben darf.



Die Verkabelung und die Konfiguration der Switchports in das VoIP VLAN müssen vom Kunden bereitgestellt werden.

Der Vorteil dieser Variante ist deren Einfachheit

Hinweis: Softclient mit VoIP Funktion (Desktop Communicator, Desktop Operator) können hier nicht eingesetzt werden.



Variante B: Getrennte AIC Infrastruktur mit VLAN

Variante C: Gemeinsame AIC Infrastruktur

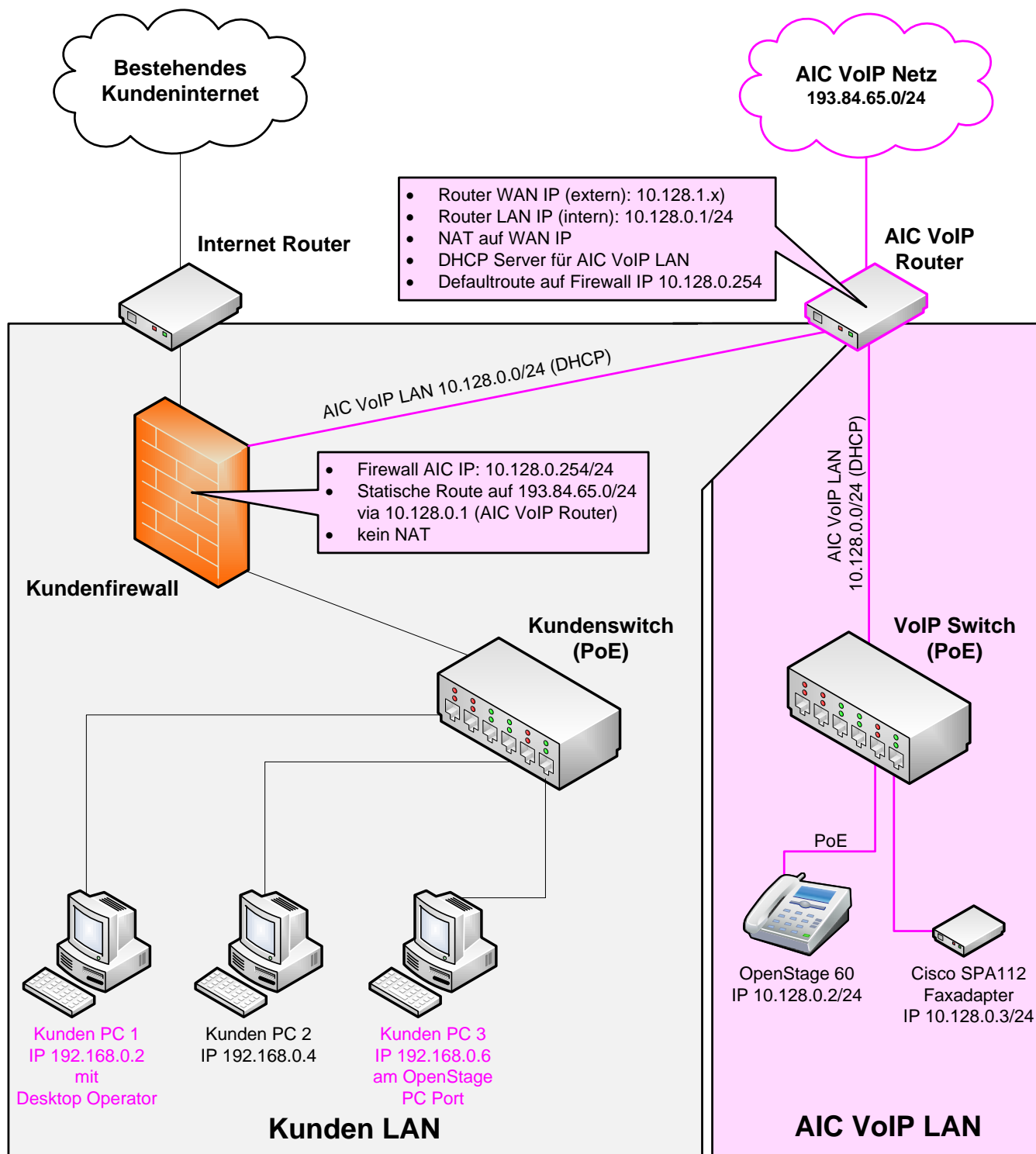
In dieser Variante wird der AIC VoIP Router mit dem Kundenrouter oder der Kundenfirewall verbunden. Die VoIP Endgeräte befinden sich im Kunden LAN und sind in diesem auch von jedem Arbeitsplatz erreichbar. Die Firewall des Kunden muss über



DAS VERBINDET UNS.

einen eigenen Anschluss mit dem AIC VoIP Router verbunden werden. In Richtung dieses Gateways muss diese Firewall IP Netze, wie im Anhang genannt, über diesen Anschluss routen. Umgekehrt muss der AIC VoIP Router im LAN mit den IP Adressen 10.128.0.0/24 (oder alternativ 172.31.0.0/24), sowie die Plattform IP Adressen (siehe Anhang) im Kunden-LAN erreichbar sein.

Um Softclients (Desktop Operator, Desktop Communicator) und VoIP Telefone betreiben zu können wird die hier beschriebene Variante benötigt, um die Netzwerkkommunikation aus dem Kunden LAN zum AIC VoIP Netz zu ermöglichen.



Variante C: Gemeinsame AIC Infrastruktur mit Softclients

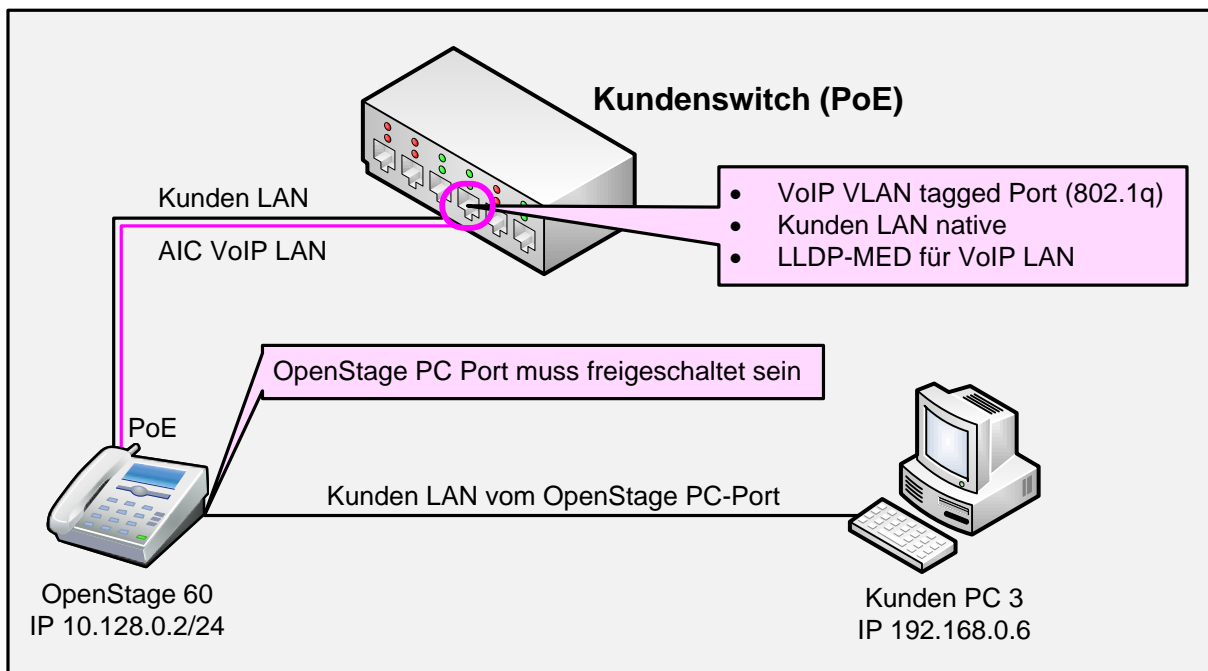


Sonderfall PC hinter VoIP Telefon

In Sonderfällen ist es durch Einschränkungen in der Verkabelung notwendig, den PC des Arbeitsplatzes hinter das Telefon zu hängen und somit einen Netzwerk-Anschluss einzusparen. Diese Konfiguration ist nur mit Variante B und C möglich.

Es gilt hier einige Besonderheiten zu berücksichtigen:

- Das Switchport des Telefons muss mit dem VoIP VLAN konfiguriert werden (tagged, 802.1q)
- Das PC-LAN läuft native auf diesem Port
- LLDP-MED mit VoIP-VLAN Konfiguration ist empfohlen, um das Telefon entsprechend in das VoIP-VLAN zu bringen
- Alternativ kann nur eine manuelle Konfiguration durchgeführt werden, die bei jedem Telefonausch wiederholt werden muss



Sonderfall PC hinter Telefon

Zusätzliche Anforderungen an das Netzwerk

Firewall Regeln

Die Kundenfirewall soll jeglichen Verkehr von der „Inside“ (Kunden LAN) zur VoIP VPN „Outside“ (AIC Plattform) erlauben. Die VoIP VPN „Outside“ kann auf die im Anhang genannten IP Netze eingeschränkt werden.

Um die Unterstützung für Path MTU Discovery (PMTU) zu gewährleisten, müssen unbedingt alle ICMP Nachrichten, vor allem „ICMP cannot fragment“, von der Firewall in beide Richtungen durchgelassen und geroutet werden.

Die Firewall Regeln sind:

„Inside“ → AIC Plattform Subnet: Any IP protocol (ICMP, UDP, TCP)



AIC Plattform Subnet → "Inside": ICMP

Sollten Security Anforderungen dies nicht erlauben, sind die verwendeten Ports und Protokolle im Anhang aufgeführt. Bei Fehlverhalten ist jedoch diese einfache Regel zu installieren, um Probleme auf der Firewall auszuschließen!

Es ist zwingend erforderlich, dass die Firewall keine wie auch immer gearteten Manipulationen durch Deep Inspection oder andere Mechanismen (Application Layer Gateway) an den Protokollen SIP und HTTP vornimmt. D.h. es sind die nachstehenden Mechanismen (oder andere ähnliche) zumindest für das LAN, in dem sich die VoIP Telefone befinden, zu deaktivieren:

- Deep Inspection
- UDP Port Hopping
- SIP Awareness / SIP NAT Support / SIP ALG
- HTTP Content Filtering

Verwendete IP Adressen

Im All In Communication Netzwerk werden private IP Adressen aus den Bereichen 10.128.0.x bzw. 172.31.0.x vergeben.

Das Verbindungsnetz zwischen Kundenfirewall und T-Mobile AIC VoIP Router wird standardmäßig mit den IP Adressen 10.128.0.0/24 konfiguriert. Falls dieses Subnet bereits in Verwendung ist, wird von T-Mobile nach Rücksprache alternativ das Subnet 172.31.0.0/24 konfiguriert.

Das Ethernetport des AIC VoIP Routers darf nicht direkt mit dem Kunden LAN verbunden werden, da der AIC VoIP Router ebenfalls IP Adressen via DHCP auf diesem LAN vergibt (DHCP Server) und damit Konflikte mit der Kundeninfrastruktur entstehen.

Der AIC VoIP Router ist standardmäßig mit der IP Adresse 10.128.0.1 oder alternativ mit 172.31.0.1 konfiguriert.

Die Kundenfirewall muss mit der IP Adresse 10.128.0.254 oder alternativ mit 172.31.0.254 konfiguriert werden. Für redundante Firewall Konfigurationen stehen auch die IP Adressen 10.128.0.252 und 10.128.0.253 (oder alternativ 172.31.0.252 und 172.31.0.253) zur Verfügung.

Switched LAN Umgebung (< 30 bis 50 Arbeitsplätze)

Dies betrifft Kundenstandorte mit flacher Netzwerkinfrastruktur, in der Regel mit weniger als 30-50 Arbeitsplätzen. Das heißt, es ist ein LAN-Segment vorhanden, in dem alle Arbeitsplatz-PCs in einem IP-Subnet hängen. Die Server des Standortes liegen entweder auch in diesem Subnet oder in einer durch eine Firewall oder Router getrennten Zone.

Es wird empfohlen, die VoIP-Endgeräte ebenfalls im LAN-Segment der Arbeitsplatz-PCs unterzubringen. Dabei sind folgende Anforderungen zu berücksichtigen:

- Ein DHCP Server muss vorhanden sein: Die Telefone benötigen einen DHCP Server, der ihnen dynamische IP Adressen zuweist.
- DHCP Server Lease Times und ausreichend IP Adressen: Ein DHCP Server muss ausreichend IP Adressen zur Verfügung stellen. Die Lease Time muss entsprechend angepasst werden, um Leases von Endgeräten, die nur kurzfristig im LAN angeschlossen werden, wieder zu entfernen, bevor alle IP Adressen vergeben sind.
- DHCP Server Options: Je nach eingesetzter Hardware (Unify OpenStage, Cisco SPA) sind unterschiedliche DHCP Server



Optionen wünschenswert (siehe Anhang). Können diese nicht verwendet werden (weil sie bspw. für andere Zwecke genutzt werden), so sollten die Geräte direkten Zugang zum Internet via HTTP und HTTPS haben.

- Eigene LAN-Verkabelung zu den VoIP-Endgeräten: Es wird empfohlen, eine eigene LAN-Verkabelung zu den Telefonen bereitzustellen. Optional können die Telefone auch vor die Arbeitsplatz-PCs geschaltet werden. Dabei ist zu berücksichtigen, dass nicht bei allen VoIP-Telefonen eine Gigabit Unterstützung gegeben ist.
- Ist der Arbeitsplatz-PC mit 100 Mb/s oder weniger (über ein Telefon) angebunden, ist eine QoS Unterstützung mittels COS im LAN-Switch zwingend erforderlich. Sollte der LAN-Switch nicht mittels DSCP und/oder TOS Werten die Priorisierung am Teilnehmer-Port vornehmen können, ist ein eigenes VLAN für die VoIP-Endgeräte notwendig (siehe nachstehende QoS Anforderungen).
- Broadcasts mit hoher Bandbreite nur bei durchgängiger Gigabit Infrastruktur: Werden Applikation im Kunden LAN eingesetzt, die über Broadcasts (oder Multicast ohne IGMP Unterstützung in den Switches) kommunizieren (bspw. Video Streaming), müssen diese Broadcasts in einem vom VoIP-Verkehr getrennten VLAN separiert werden, um nicht auf Ports mit geringer Bandbreite den VoIP-Verkehr zu blockieren.
- Eine IP MTU Size von 1500 Byte ist durchgängig zu gewährleisten.
- Switches müssen auf den Ports eine korrekte automatische Erkennung von Duplex und Speed durchführen. Die VoIP Endgeräte sind auf auto/auto konfiguriert.
- Traffic Shaper dürfen den VoIP Verkehr nicht beeinträchtigen bzw. benachteiligen. Somit darf kein „Shaping“ appliziert werden und im besonderen keine „Policy“ (Packet Drops bei Rate Limit Überschreitung) verwendet werden. Bei Einsatz eines Shapers ist eine Priorisierung ohne Begrenzung für VoIP Signalierung und Media zwingend erforderlich

LAN Umgebung (> 50 Arbeitsplätze)

Dies betrifft Kundenstandorte mit vielen Arbeitsplätzen, die auf mehrere LAN-Segmente verteilt sind und wo ein Layer 3 Router diese Segmente miteinander verbindet.

Grundsätzlich gelten hier die gleichen Anforderungen wie in flachen Netztopologien (siehe oben). Eine zusätzliche Anforderung ist, dass der Router zwischen den Segmenten eine ausreichende Performance aufweist, um kleine Pakete (RTP) routen oder switchen (Layer 3 Switch) zu können. Bei Anschluss-Bandbreiten kleiner 1 Gb/s des Routers an die LAN Segmente muss eine Priorisierung der VoIP-Pakete, zumindest der TOS5 (DSCP 184=EF und 160=CS5) markierten Pakete, erfolgen.

VoIP VLAN

Alternativ kann bei größeren Installationen auch ein eigenes VoIP VLAN in einer reinen Switching Infrastruktur aufgespannt werden, wobei hier die Anforderungen der „Switched LAN Umgebung“ zum Tragen kommen (siehe oben). Werden dabei Telefone zwischen PC und Switch geschaltet (VoIP VLAN tagged), können aktuell nur Hardphones in dieses VLAN aufgenommen werden. Softphones auf den Arbeitsplatz-PCs unterstützen kein VoIP VLAN tagging.

VoIP VLAN Zusatzanforderungen

Wird ein VoIP VLAN vorgesehen und dieses als tagged VLAN ausgeführt (Telefon zwischen PC und Switch ohne eigene Verkabelung), gilt zu beachten, dass für die Funktion der automatischen Provisionierung ein Hardphone auch im regulären VLAN des Arbeitsplatz-PCs einen Zugang zum Internet via HTTP und HTTPS (ohne HTTP(S) Proxy) benötigt oder mit entsprechenden DHCP Settings (siehe Anhang) versorgt wird. Dies ist nur für die initiale Provisionierung (und nach gegebenenfalls erforderlichem Factory Reset des Hard Phones) notwendig. Hat das Hardphone einmalig den Config Server (via HTTP(S)) erreicht, so erfolgt die weitere Provisionierung und auch der Regelbetrieb über das VoIP VLAN. Dies gilt es in den



Firewalls und Routern zu berücksichtigen.

Bei Einsatz eines VoIP VLANs ist darauf zu achten, dass End2End eine IP MTU Size von 1500 Byte verfügbar ist und Switching Equipment keine Pakete aufgrund zu großer Paketlänge verwirft!

Es wird nur VLAN Tagging nach IEEE 802.1Q unterstützt.

Quality of Service (QoS) Funktionen im LAN Switch

Um die Qualität im LAN sicherzustellen, gibt es zwei Methoden:

- Ausreichend Bandbreite: Wird die komplette Infrastruktur des Kundenstandortes durchgängig mit Gigabit LAN umgesetzt, ist keine weitere QoS Unterstützung gefordert, aber dennoch empfohlen.
- QoS Unterstützung und saubere Konfiguration der PC Clients: Die LAN Infrastruktur und die eingesetzten Layer 3 Switches müssen DiffServ Code Points (DSCP) von Endgeräten vertrauen (DSCP trusted) und diese in Class-of-Service (COS) übernehmen.

Wird QoS/CoS Unterstützung in den LAN Switches konfiguriert, so sind folgende DSCP / TOS Werte in die Priority Queues der LAN Switches einzuordnen und „normale“ PC Clients derart zu konfigurieren, dass diese nicht „unbeabsichtigt“ Datenverkehr mit diesen DSCP Werten versenden:

RTP Traffic: DSCP 184 (dec) / 46 (0x2E) / EF und DSCP 160 (dec) / 40 (0xa0) / CS5 (mapped into CoS 5) matching to Strict Priority Queue

VoIP Signalling: DSCP 128 (dec) / 32 (0x20) / CS4 und 136 (dec) / 34 (0x22) / AF41 (mapped into CoS 4) matching to non-default queue

Wird RTP Verkehr in die Strict Priority Queue eingeordnet, so ist zu beachten, dass manche Hersteller diese mit 1/25 der Linkbandbreite limitieren (bspw. 4Mb/s bei 100 Mb/s). Dies muss berücksichtigt werden, wenn mehr als 40 VoIP Endgeräte über einen 100 Mb/s oder 4 Geräte über einen 10Mb/s Link angebunden werden (Use Case: Default Setting bei Verwendung von Cisco „mls qos“ in Enterprise Switches).

LAN QoS Anforderungen (RoundTripDelay, Jitter, Packet-Loss): < 10 ms / < 10 ms / < 0.25% (ohne Packetization Delay, reine Round-Trip Time)

Einstellung bei Verwendung eines Faxgerätes

- Faxgeräte müssen auf eine maximale Geschwindigkeit von 14.400 bps (V.17) eingestellt werden.
- Der ECM (Error correction mode) soll aktiv sein.
- Es wird nur das MFV (Mehrfrequenzwahlverfahren) unterstützt (kein Impulswahlverfahren).

Bei Verwendung eines Faxgerätes, das 33.600 (V.34) unterstützt, kann ein störungsfreier Betrieb nicht gewährleistet werden.



Anhang

Plattform Kommunikation

All In Communication Plattform IP Adressen (IP Netz über AIC VoIP Router zu routen): 193.84.65.0/24

All In Communication Plattform Ports:

DNS Name	IP	Protokoll/Port	Beschreibung
conf.aic.t-mobile.at	193.84.65.8	TCP:443 (https) TCP:80 (http) TCP:8080 (http) UDP:69 (tftp) TCP:18443 (https)	Autoprovisioning, Phonebook
aic.t-mobile.at	213.208.137.170 193.84.65.9	TCP:443 (https)	AIC Provisioning Portal Provisioning für Softclients
sip.aic.t-mobile.at	193.84.65.16	UDP:5082 (SIP) UDP:5083 (SIP) UDP:5075 (SIP) UDP:10000-19999 (RTP)	VoIP Telefonie
em.aic.t-mobile.at	193.84.65.50	TCP:443 (https) TCP:80 (http)	Element Manager

Softclients DesktopControl und DesktopOperator

Folgende Systemanforderungen sind zu erfüllen:

	Minimum	Empfohlen
CPU	1.6 GHz Intel Pentium oder kompatibel	2.0 Ghz Intel Core i3 oder kompatibel
Memory	1024 MB	2048 MB
Graphiksystem		
DesktopControl	800x600	1366x768
DesktopOperator	1024x768	
Audiosystem	Standard Windows Soundsystem	USB-Headset
Network	100Mbit Ethernet, QoS settings für VoIP-Betrieb empfohlen	
Benötigter Festplattenspeicher	200 Mbyte	

Hinweis: Um die Kommunikation mit dem AIC VoIP Netz zu ermöglichen, muss eine Netzverbindung, wie in Variante C beschrieben, umgesetzt werden!



DAS VERBINDET UNS.

Unterstützte Betriebssysteme:

- Windows XP SP3 32 bit
- Windows Vista SP2 32 bit
- Windows 7 SP1 32/64 bit
- Windows 8 32/64 bit

Hinweis: Terminal Server Funktion wird aktuell noch nicht unterstützt.

Benötigte Sicherheits-Einstellungen:

- Zur Installation der Software unter Windows sind Administrator-Rechte notwendig.
- Die Software muss das Netzwerk ausgehend benutzen dürfen und öffnet mindestens einen Netzwerkport.

Die Clients benötigen am Kunden PC Zugang zu folgenden Zielen:

- Provisioning: 193.84.65.9 (http/https)
- Telefonie: 193.84.65.16 (sip/5082, sip/5075)

Torsprechanlagen, Türöffner und automatische Schrankenanlagen

Grundsätzlich können solche analogen Endgeräte über einen Analogadapter angeschaltet werden. Es werden ein freier analoger Port sowie ein eigener Teilnehmer mit Durchwahl benötigt. Über DTMF (Dual tone multi frequency) können Aktionen an das Endgerät übermittelt werden. Wenn das Endgerät SIP unterstützt kann die Anschaltung alternativ auch direkt per SIP erfolgen. Der Übergabepunkt an den Kunden ist entweder das analoge Port des Analogadapters oder die SIP Schnittstelle.

Sobald ein derartiges Endgerät angeschaltet werden soll, ist der technische Ansprechpartner von T-Mobile zu kontaktieren. Das weitere Vorgehen wird dann mit dem technischen Ansprechpartner des Kunden abgestimmt. Etwaig notwendige Konfigurationsänderungen an dem jeweiligen Endgerät sind vom technischen Ansprechpartner des Kunden durchzuführen.

VPN Verbindungen im Kunden LAN

VPN Verbindungen im Kunden LAN sind nicht unterstützt!

Sind VPN Verbindungen bereits mit entsprechender Qualität und Bandbreite im Einsatz, ist ein Betrieb von Telefonen grundsätzlich in eigener Verantwortung des Kunden möglich. Für die Störungseinsmeldung ist in diesem Fall das Problem im AIC VoIP LAN nachzuweisen.

DHCP Optionen für Telefone außerhalb des AIC VoIP LAN

Die notwendigen Basis-Einstellungen für die Telefone und Analogadapter werden vom AIC Router automatisch im AIC VoIP LAN mittels DHCP verteilt. In Sonderfällen kann es vorkommen, dass Telefone direkt im Kunden LAN betrieben werden müssen.

Um auch hier eine automatische Provisionierung bei neuen Geräten, Gerätetausch oder Zurücksetzen der Geräteeinstellungen zu ermöglichen, müssen nachstehende DHCP Optionen in jedem Netzbereich in dem Telefone oder Adapter genutzt werden vom jeweiligen DHCP Server bereitgestellt werden. Die Konfiguration obliegt hier dem Kunden selbst.



DHCP Optionen für Cisco/Panasonic/Snom

```
option boot-server code 66 = string;      # standard option 66
option boot-filename code 67 = string;    # standard option 67

option boot-server "conf.aic.t-mobile.at";
option boot-filename "";
```

DHCP Optionen für Unify OpenStage Telefone

Unify OpenStage SIP Telefone benutzen eine Vendor Specific Encapsulation in DHCP Option 43.

DHCP Option 43 fields:

- Option 01 (10 bytes): Magic-Code identifying Vendor-String = "Siemens" padded with 3 zeros:
53:69:65:6D:65:6E:73:00:00:00
- Option 02 (4 bytes): VLAN-Id in hexadecimal notation (e.g. 00:00:00:0a for VLAN 10)
- Option 04 (variable): DLS Server with FQDN (e.g. sdlp://conf.t-mobile.at:18443)

Beispiel ISC DHCPd:

```
option space OptiIpPhone;
option OptiIpPhone.magic code 1 = string;
option OptiIpPhone.vlanid code 2 = unsigned integer 32;
option OptiIpPhone.dlsip code 3 = string;
option OptiIpPhone.dls code 4 = string;

vendor-option-space OptiIpPhone;
option OptiIpPhone.magic      53:69:65:6D:65:6E:73:00:00:00;
                              # "SIEMENS\0\0\0"
option OptiIpPhone.vlanid     0;
option OptiIpPhone.dls        "sdlp://conf.aic.t-mobile.at:18443";
```

Beispiel Cisco IOS:

```
ip dhcp pool my-voip
  network 192.168.37.0 255.255.255.224 ! example!
  default-router 192.168.37.1         ! example!
  option 43 hex
010a.5369.656d.656e.7300.0000.0204.0000.0000.0421.7364.6c70.3a2f.2f63.6f6e.662e.6169.632e.742d.6d6f.62
69.6c65.2e61.743a.3138.3434.33ff
```

DHCP Optionen für Cisco (Linksys) Analog terminal adapter (ATA)

```
option option-160 "http://em.aic.t-mobile.at/";
option boot-server "conf.aic.t-mobile.at";
option boot-filename "";
```

