Application Note

Fernsteuerung von MXE5 mit Inter-VLAN-Routing und ACLs

MXE Matrix Mix Engines sind mit einem OMNEO Dante OCA-Netzwerkinterface für die Verbindung zu anderen Systemen, unter Verwendung von CAT-Kabeln und Ethernet-Netzwerk-Switches, ausgestattet.

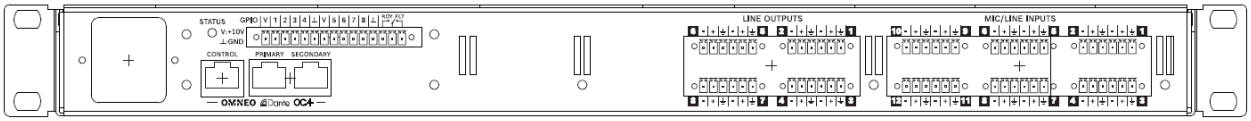


Bild 1: MXE-Rückansicht

Das Netzwerk-Interface (*OMNEO Dante OCA*) befindet sich auf der MXE-Rückseite. Es bietet insgesamt drei Netzwerk-Ports: *CONTROL*, *PRIMARY* und *SECONDARY*.

Die drei Netzwerk-Ports können über die SONICUE Software für Transparent-, RSTP- oder Glitch-Free-Modus konfiguriert werden.

Der *CONTROL*-Port überträgt immer dieselben Daten wie der *PRIMARY*-Port, mit Ausnahme von Dante Multicast-Audiodaten, die gefiltert werden. Dies macht ihn ideal für die Verbindung mit einem WiFi-Accesspoint, oder generell für reine Bediengeräte, allerdings nicht für die Verbindung zu einem dedizierten Control VLAN (Virtual Local Area Netzwerk) – in diesem Fall fungiert er als Brücke(!) zum OMNEO/Dante-Netzwerk.

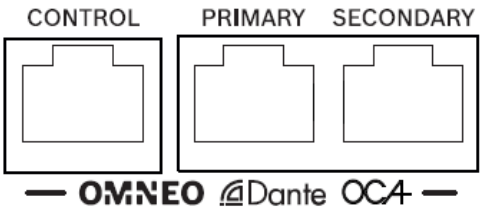


Bild 2: MXE-Netzwerkinterface Detailansicht

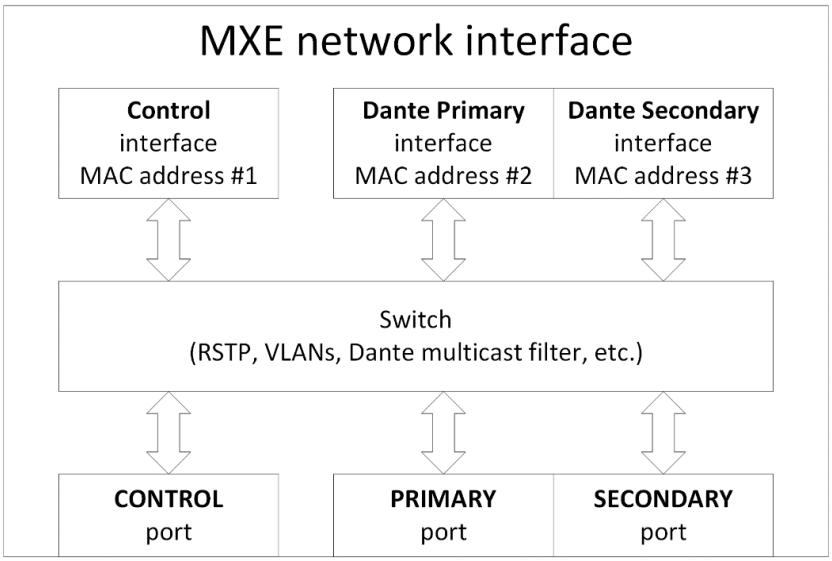


Bild 3: MXE-Netzwerkinterface Blockdiagram

MXE-Netzwerkinterface – *Transparent*-Modus

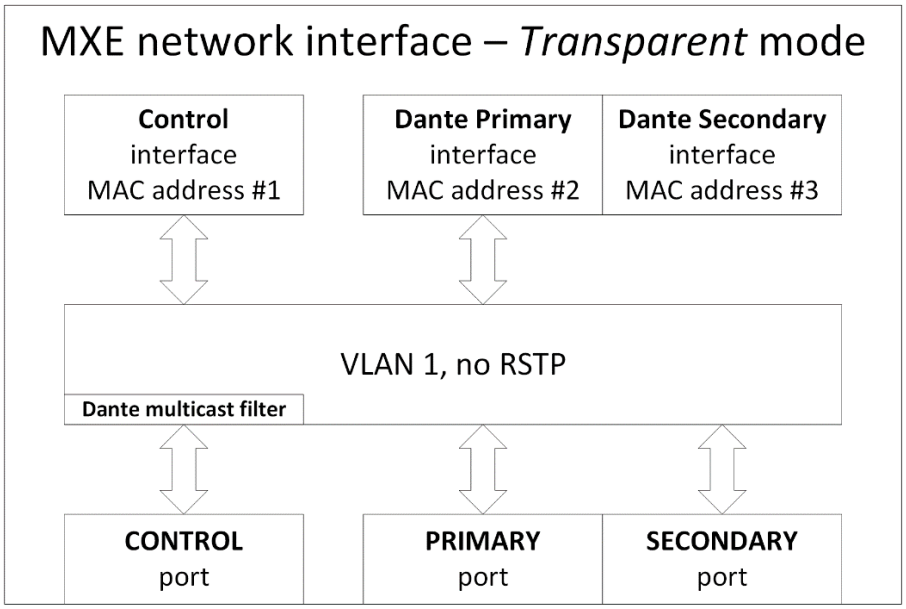


Bild 4: MXE-Netzwerkinterface – Transparent-Modus

MXE-Netzwerkinterface – *RSTP*-Modus

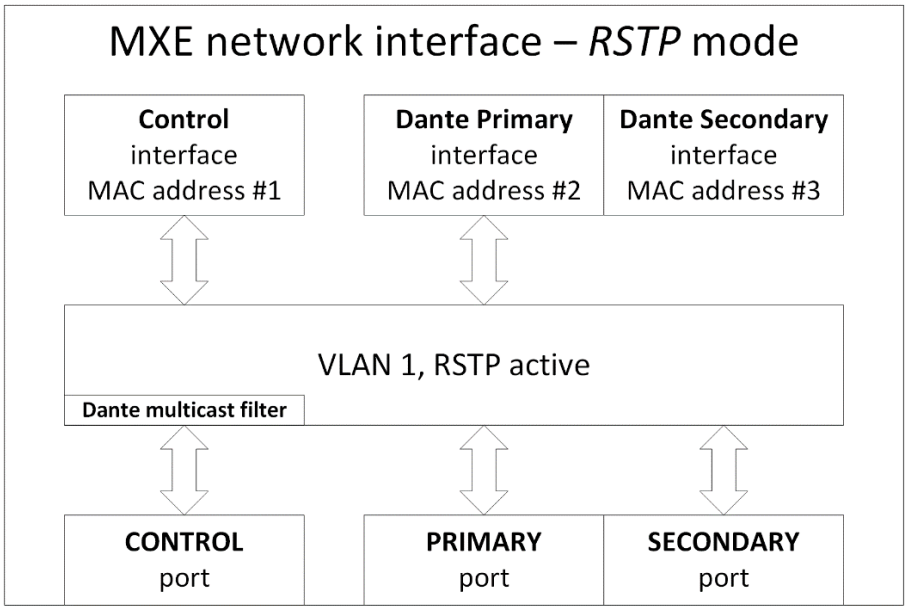


Bild 5: MXE-Netzwerkinterface – RSTP-Modus

MXE-Netzwerkinterface – *Glitch-Free*-Modus

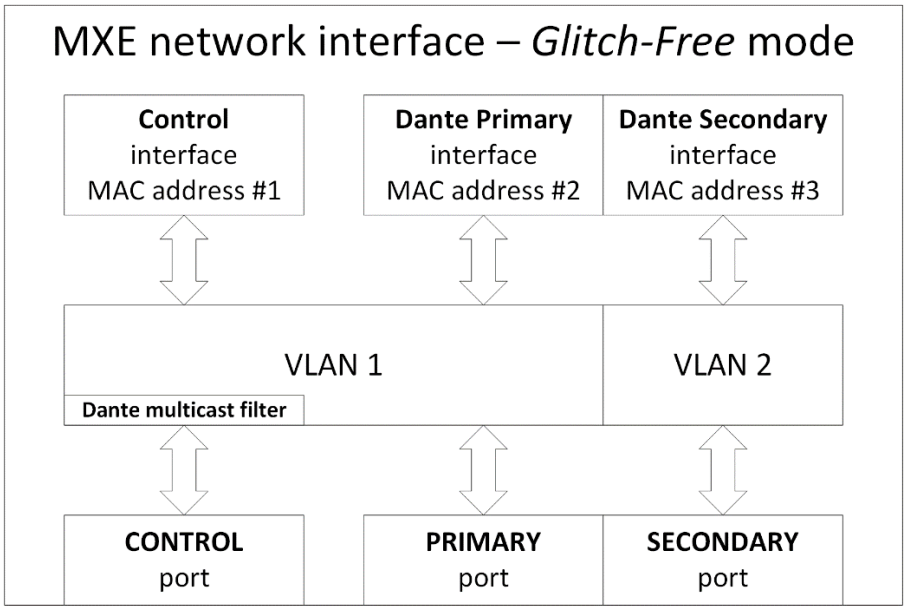


Bild 6: MXE-Netzwerkinterface – Glitch-Free-Modus

OMNEO und Netzwerksicherheit

OMNEO ist eine Kombination von Audio- und Steuerdaten, was zahlreiche Vorteile bietet. Je nach Projekt-Anforderungen ist es möglich, Audio- und Steuerdaten effizient zu verwalten und zu trennen. Zum Beispiel um ein AV-Netzwerk strukturiert zu gestalten und Interferenz mit anderen Systemen, wie z.B. Video-, Licht- oder Kassensystem zu vermeiden.

Aus Gründen der Netzwerksicherheit sollten OMNEO-Geräte stets über ein dediziertes VLAN vom Internet (www) getrennt, und zusätzlich über eine Access Control List (ACL) geschützt werden.

Diese Application Note beschreibt am Beispiel einer MXE5 Matrix, eines Cisco CBS-350-Switches und eines AVM FRTIZ!Box DSL-Routers, wie man OMNEO-Geräte via separatem VLAN isoliert, dieses über ACL schützt, und zugleich Steuer-Zugriff von außerhalb dieser geschützten „Insel“ gewährt.

Für eine vollumfängliche Übersicht der möglichen Netzwerksicherheits-Maßnahmen, für MXE und ein verbundenes SONICUE-Ökosystem, lesen Sie bitte das *MXE Security Precautions.pdf* (enthalten in allen SONICUE-Downloadpaketen).

Anforderungen, um SONICUE Control in Verbindung mit MXE Control Server mit statischer IP und MXE mit festen Ports zu verwenden:

MXE Matrix Mix Engine mit Firmwareversion 1.6.3342 (oder höher)

SONICUE Sound System Software 1.4.0 (oder höher) installiert auf dem Computer

MXE Control Server

Die MXE Matrix Mix Engine ist das zentrale Gerät im SONICUE-Ökosystem, und verdient daher spezielle Aufmerksamkeit.

Auf der MXE läuft der Control Server, der die OCA-Befehle -verwendet für die Kommunikation der OMNEO-Geräte untereinander- in Web-Socket-Befehle für die Kommunikation mit SONICUE-Bedieneinheiten (wie dem WPN1 Wall-Panel, dem TPC-1 Touch-Panel, oder iOS-Geräten und Windows-PCs, auf denen die SONICUE Control App läuft).

MXE Control Server – Ports

Wenn eine Access Control List (ACL) konfiguriert werden soll ist es wichtig die Ports zu kennen, die durch die Access Control List gelassen werden sollen:

- Für Control Server-Kommunikation verwendet die MXE den Port 27999.
- Für OCA-Kommunikation verwendet die MXE den Port 55555.

Der Port 55555 ist primär in Kombination mit Crestron- oder Q-Sys-Steuerungen relevant, welche sich in einem separaten VLAN befinden, da die Crestron- und Q-Sys-Plug-Ins auf dem OCA-Protokoll basieren.

SONICUE ControlServer Discovery

Per Default finden sowohl die SONICUE Software als auch die SONICUE Control App Geräte via mDNS und nutzen Gerätenamen für die Kommunikation. Die von mDNS dafür verwendete Multicast IP-Adresse (224.0.0.251) ist per Definition der IEEE nicht routbar.

Wenn Bediengeräte über ein dediziertes Control-VLAN von OMNEO/Dante-Geräten separiert werden sollen, muss die Kommunikation auf IP-Adressen basierend sein und der Netzwerk-Switch muss IP-Routing (Layer 3-Modus) unterstützen.

Der SONICUE Panel Designer bietet eine Option, um die *ControlServer Discovery*-Methode zu definieren.

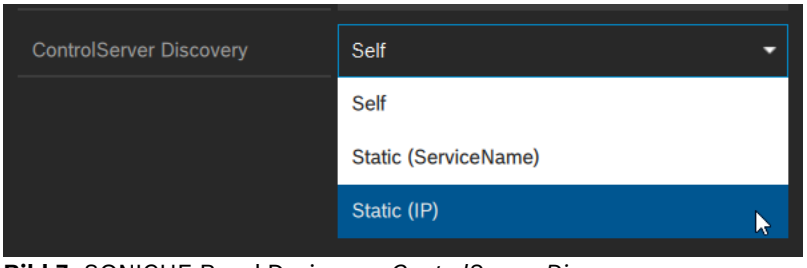


Bild 7: SONICUE Panel Designer – *ControlServer Discovery*

Per Default ist die *ControlServer Discovery* auf Auto oder *Self* (abhängig vom Gerät) eingestellt, aber sie kann alternativ auf *Static (Service Name)* oder *Static (IP)* eingestellt werden.

Die *Static (IP)*-Option muss verwendet werden um SONICUE-Bediengeräte, wie das WPN1 Wall Panel, TPC-1 Touch Panel, oder iOS-Geräte und Windows-PCs, auf denen die SONICUE

Control App läuft, über ein dediziertes Control VLAN von OMNEO-Geräten, wie MXE Matrix Mix Engines und einem verbundenen SONICUE-Ökosystem, zu trennen.

Für die initiale Konfiguration müssen alle Geräte mit demselben Netzwerk verbunden sein wie der PC, auf dem die SONICUE Software für Systemdesign und -konfiguration läuft. Nachdem die Bediengeräte ihre gewünschte Konfiguration erhalten haben, können sie mit einem separaten VLAN verbunden werden.

Testsystem für Inter-VLAN-Routing und ACLs

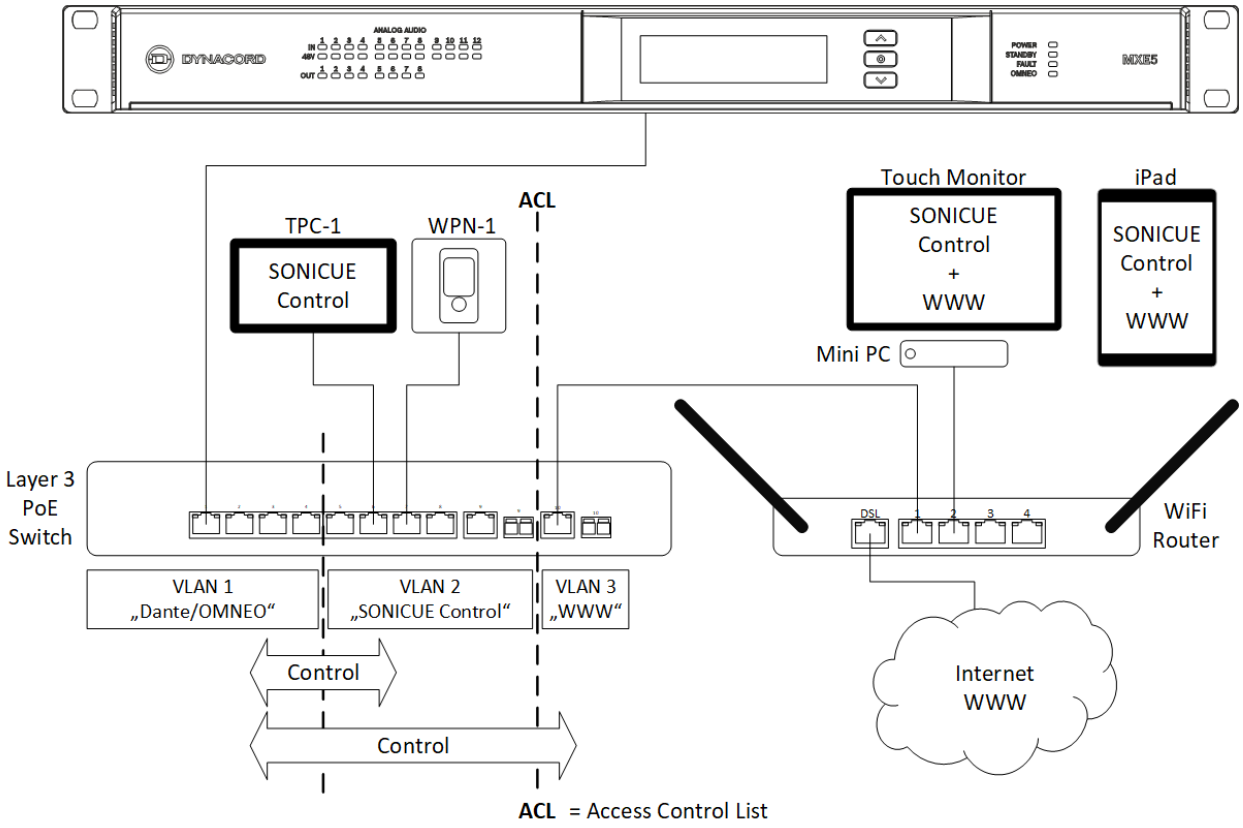


Bild 8: Testsystem für Inter-VLAN-Routing and ACLs

Kurze Beschreibung des Testsystems

Die Idee hinter diesem Testsystem ist es, alle Audiogeräte in einem VLAN, und alle Bediengeräte in (einem) anderen VLAN(s) zu betreiben.

- Audio existiert nur in VLAN 1.
- Steuerdaten (Control) werden zu den VLANs 2+3 geroutet.

- VLAN 1 wird für alle Dante- und OMNEO-Geräte mit Dante Audio verwendet.
- VLAN 2 wird für Bediengeräte verwendet, die von Audiogeräten getrennt sein sollen.

- VLAN 3 wird für Bediengeräte verwendet, die von Audiogeräten getrennt sein sollen und zusätzlich Internetzugang benötigen.

Der MXE Control Server sorgt für die Kommunikation zu den Bediengeräten in VLAN 2+3, und dient zugleich als „Gateway“ zum VLAN 1, wo auch andere OMNEO-Geräte -wie IPX- oder TGX-Verstärker- verbunden werden können.

IP-Adressen die im Testsystem verwendet werden

- VLAN 1
  - Die MXE5 nutzt eine fixed-IP 192.168.1.110 -> Dies ist der Control Server
  - Andere Geräte, die mit VLAN 1 verbunden sind, erhalten die IP-Adresse aus dem VLAN 1-DHCP-Pool 192.168.1.1…100
- VLAN 2
  - Das TPC-1 und WPN-1 erhalten ihre IP-Adresse aus dem VLAN 2-DHCP-Pool 192.168.2.1…100
  - Andere Geräte, die mit VLAN 2 verbunden sind, erhalten ihre IP-Adresse ebenfalls aus dem VLAN 2-DHCP-Pool 192.168.2.1…100
  -
- VLAN 3
  - Der DSL-Router nutzt eine fixed-IP 192.168.178.1 -> Dies ist das Gateway ins Internet (www)
  - Das iPad und der Mini-PC erhalten ihre IP-Adresse aus dem DSL-Router-DHCP-Pool 192.168.178.2…100
  - Andere Geräte, die mit VLAN 3/DSL-Router verbunden sind, erhalten ihre IP-Adresse ebenfalls aus dem DSL-Router-DHCP-Pool 192.168.178.2…100

Private IP-Adressen

Die folgenden, so genannten privaten IP-Adressbereiche werden für die Verwendung in einem SONICUE-Ökosystem empfohlen. Idealerweise werden diese IP-Adressen von einem DHCP-Server zugewiesen, können aber bei Bedarf auch als statische IP-Adressen manuell zugewiesen werden. All diese IP-Adressen sind zwischen Subnetzen/VLANs routbar.

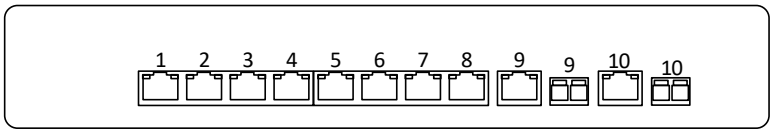
- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

Link-Local-IP-Adressen

Per Default, wenn kein DHCP-Server vorhanden ist und auch keine statische IP-Adresse manuell zugewiesen wurde, verwenden Dante- und OMNEO-Geräte automatisch IP-Adressen aus dem Link-Local-Bereich. Link-Local-IP-Adressen werden nicht gerouted, so dass sie in dem Szenario, das in dieser Application Note beschrieben wird, nicht verwendet werden können.

- 169.254.0.0/16

Switch-Konfiguration



VLAN 1 „Dante/OMNEO“	VLAN 2 „SONICUE Control“	VLAN 3 „WWW“

Bild 9: PoE-Switch – VLAN-Netzwerke

Für den Test verwendeter Switch: Cisco CBS350-8P-E-2G-EU (10-Port, PoE)

- Basic OMNEO-Konfiguration (RSTP, QoS, EEE aus, etc.)

- IP-Routing aktiviert (-> Layer 3-Switch)

- VLANs
    - VLAN 1
        - Ports 1-4
        - IP-Interface 192.168.1.254/24 (dies ist auch das Gateway im VLAN 1)
        - DHCP-Pool 192.168.1.1…100/24
    - VLAN 2
        - Ports 5-9
        - IP-Interface 192.168.2.254/24 (dies ist auch das Gateway im VLAN 2)
        - DHCP-Pool 192.168.2.1…100/24
    - VLAN 3
        - Port 10
        - IP-Interface 192.168.178.254/24 (dies ist nicht das Gateway im VLAN 3)
        - Gateway 192.168.178.1

- Access Control List (ACL)
    - ACE (ACL Extended)
        - Priority 10 Permit TCP from IP 192.168.1.110, wildcard 0.0.0.0, Port 27999 to 192.168.178.1, wildcard 0.0.0.255 (= von MXE mit fixed-IP zu jeder IP im Router-Netzwerk 192.168.178.1/24)
        - Priority 20 Permit TCP from 192.168.178.1 wildcard 0.0.0.255 to IP 192.168.1.110, wildcard 0.0.0.0, Port 27999 (= von jeder IP im Router-Netzwerk 192.168.178.1/24 zur MXE mit fixed-IP)
        - Deny any (per Default am Ende einer ACE, blockt allen anderen Traffic)
    - ACL Binding
        - auf Interface 10 (Port 10)
        - als IN und OUT
    - MXE5-Ports die durch die ACL gelassen werden sollen:
        - 27999 für MXE-Steuerdaten via Control Server
        - 55555 für MXE-Steuerdaten via OCA-Protokoll (nicht genutzt im Testsystem)

DSL-Router-Konfiguration

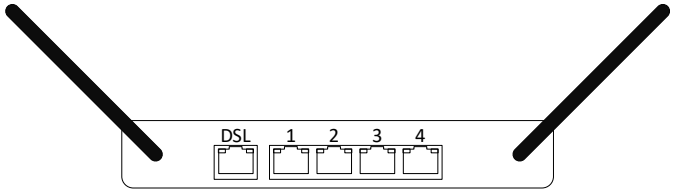


Bild 10: DSL-Router

Für den Test verwendete DSL-Router: AVM FRITZ!Box 7530 und AVM FRITZ!Box 6820 LTE

- Default-Konfiguration:
  - IP-Adresss 192.168.178.1/24
  - DHCP-Pool 192.168.178.2…100/24

- Konfiguration die vom User gemacht werden muss:
  - Statische Route 1:
    - Netzwerk 192.168.1.0/24
    - Gateway 192.168.178.254
  - Statische Route 2 (optional):
    - Netzwerk 192.168.2.0/24
    - Gateway 192.168.178.254
    - Nur dann nötig, wenn sich zu steuernde Geräte (3rd-Party-Zubehör) in VLAN 2 befinden

Haftungsausschluss für Produkte Dritter:

Dynacord übernimmt keine Verantwortung für Garantie, Qualität, oder Verfügbarkeit von Cisco- und AVM-Produkten. Die in diesem Dokument enthaltenen Cisco- und AVM-Produkte wurden zum Zeitpunkt der Veröffentlichung erfolgreich getestet. Jedoch kann Dynacord die Kompatibilität mit zukünftigen Modellen oder Variationen der Cisco- und AVM-Produkte nicht garantieren, da diese nicht kompatibel sein könnten. Bitte nutzen Sie die Cisco- und AVM-Webseiten für produktspezifische Informationen.