Dante Domain Manager – Information for Network Administrators

1. Overview

Dante Domain Manager (DDM) brings user authentication, role-based security and audit capabilities to Dante networks, while allowing nearly unlimited expansion and organization of Dante systems over any network topology, including routed networks. DDM comes with an intuitive and highly responsive web interface for desktop and tablet browsers.

DDM is provided as an ISO for installation on virtualization platforms or bare-metal Linux machines. It is assumed that multi-subnet systems are properly configured to allow Dante control and audio traffic between subnets.

2. Network Services

Refer to 'Bootstrapping Dante Devices' in the DDM user guide for more information about configuring network services.

2.1. Routed Networks

2.1.1. With DHCP and DNS

- Use DHCP to assign addresses to devices
- Use DNS SRV records for DDM discovery

Note: Ensure that DHCP provides devices with a DNS server address and search path (domain). You can use static IP to enroll devices, but this is not the recommended option for this network configuration.

2.1.2. With Static Addressing

- Use manual enrollment via IP address to enroll devices
- Ensure devices *and* the DDM server have static addresses

2.2. Single-subnet Networks

- In the absence of DHCP and DNS, use Link-local addressing and mDNS (Dante Discovery Service) for discovery

2.3. DHCP Configuration

- Specify the DNS domain name for the DDM as the first entry in the domain-search option

2.4. DNS Configuration

Devices and controllers use DNS-SD (DNS service discovery) to find the DDM. Each DNS-SD entry consists of an SRV record describing how to connect to the DDM and a TXT record with additional information (empty in this case).

Note that DNS domain names and Dante domain names are different, and need not be related. Names of Dante domains are not added to the DNS.

2.4.1. Customizable Fields

The following fields are customizable to your environment.

- Domain: Replace the string `my.domain.example.com` with your local domain
- DDM: Replace the string `my_ddm.my.domain.example.com` with the name of the device hosting your DDM
- TTL: The system default TTL is usually satisfactory

2.4.2. Required Fields

All other fields must be as specified below.

Controller Record

Record Name

Instance	Service	Domain
`default.`	`_dante-ddm-c._tcp`	`my.domain.example.com`

- `default._dante-ddm-c._tcp.my.domain.example.com`

SRV Record

- Weight, priority: 0
- Port: 8443
- Target: `my_ddm.my.domain.example.com`

TXT Record

- Empty

Device Record

Record Name

Instance	Service	Domain
default.	_dante-ddm-d._udp	my.domain.example.com

- default._dante-ddm-d._udp.my.domain.example.com

SRV Record

- Weight, priority: 0
- Port: 8000
- Target: my_ddm.my.domain.example.com

TXT Record

- Empty

2.4.3. DNS SRV Record Examples

The following example is for Dante **controllers**, using the domain name eng.example.com:

```
default._dante-ddm-c._tcp.eng.example.com. 3600 IN SRV 0 0 8443 ddm.eng.example.com
default._dante-ddm-c._tcp.eng.example.com. 3600 IN TXT ""
```

The following example is for Dante **devices**, using the domain name eng.example.com:

```
default._dante-ddm-d._udp.eng.example.com. 3600 IN SRV 0 0 8000 ddm.eng.example.com
default._dante-ddm-d._udp.eng.example.com. 3600 IN TXT ""
```

The domain name in the SRV and TXT headers must match the search domain provided to clients by DHCP. Clients are not required to be in the same DNS domain as the DDM, but each DNS domain provided to clients must have DNS-SD records that point to the DDM.

In addition to adding the DDM domain name to DNS, you should obtain a domain validation certificate for the hostname of your DDM. This certificate verifies the identity of your DDM to a web browser accessing the DDM administrative interface as well as Dante controllers connecting to the DDM.

Note: For Windows Server SRV record configuration, please refer to the online user guide.

3. Addresses and Ports

Dante uses UDP for audio distribution, both unicast and multicast.

3.1. Standard Ports

- mDNS and DNS-SD traffic for discovery and enumeration of other Dante devices is on 224.0.0.251:5353/UDP
- Precision Time Protocol (PTP) for time synchronization is on 224.0.1.129 - 224.0.1.132 ports 319/320/UDP

3.2. Dante Audio and Control

- Multicast audio is always on 239.255/16:4321. Unicast audio ports come from a range: 14336 - 14600/UDP
- Dante-specific monitoring traffic is on multicast addresses 224.0.0.230 - 224.0.0.233:8700-8708/UDP
- Dante devices use port 4455/UDP for audio setup

3.3. RTP (AES67 & SMPTE ST 2110-30)

- SAP/SDP is on 239.255.255.255:9875/UDP
- RTP audio is on 239.69/16:5004/UDP (address is configurable)

3.4. Dante Domain Manager

- The DDM Web interface uses HTTP on ports 80/TCP and 443/TCP
- Dante Devices connect to the DDM on port 8000/UDP
- Dante Controllers connect to the DDM on port 8001/TCP and 8443/TCP
- The LDAP default port is 389, the LDAPS default port is 636/TCP (configurable)
- The SMTP default port is 25, the SMTPS default port is 465/TCP (configurable)
- The High Availability service uses TCP on port 8081, High Availability database sync uses TCP on port 27017
- Device enrollment over IP uses UDP on port 8702

4. Outbound Access for Licensing and Online Updates

In order to activate its license, check / perform online updates and reach the user guide, the DDM instance must be able to reach Audinate's license servers at on port 443 at:

- https://software-license-ddm.audinate.com
- https://software-certificates-ddm.audinate.com
- https://software-updates-ddm.audinate.com
- https://software-links-ddm.audinate.com