OMNEO Network Requirements and Considerations

Table

of

Contents

What is OMNEO?

OMNEO is an architectural approach to connecting devices that need to exchange information such as audio content or device control. Built upon multiple technologies, including IP and open public standards, OMNEO supports the technologies of today such as Audinate's DANTE while adopting the standards of tomorrow.

OMNEO offers a professional-grade media networking solution that provides interoperability, unique features for easier installation, better performance and greater scalability than any other IP offering on the market.

Using standard Ethernet networking, media products that integrate OMNEO can be assembled into small, medium and large networks that exchange studio-quality synchronized multichannel audio and share common control systems.

OMNEO's media transport technology is based on Audinate's DANTE, a high performance standards-based, routable IP-media transport system. OMNEO's system control technology is AES70, also known as **OCA** (Open Control Architecture), an open public standard for control and monitoring of professional media network environments.

OMNEO devices are fully compatible with AES67 and AES70, without losing any functionality.

Hardware recommendation

In small intercom systems many installations make use of unmanaged switches, due to the fact it is plug and play. However, these unmanaged switches are pre-configured and cannot be modified to meet the OMNEO technical requirements in many cases. Without the possibility of modifying the settings, the device might have a default set of features enabled or disabled that cannot co-operate with the OMNEO system needs. Use this document to confirm the selected network devices conform to the requirements for OMNEO.

The use of managed professional grade switches or routers is recommended. Preferably, a switch where the features can be configured via a management interface or command line, according the OMNEO requirements. As we do not provide a white- or blacklist, we recommend researching the network equipment before purchasing additional equipment. Use this document to evaluate OMNEO network requirements with the functionality of the network device.

Cable information

To ensure disturbance-free connections between the devices, some important facts in regard to cables, connections and data transmissions must be considered.

Ethernet cables

When using Ethernet, it is most suitable to use a **CAT** (category) 5e, 6, or 6a, as these types of cables ensure improved noise rejection, reduced EMI vulnerability, and decreased crosstalk. If the Ethernet cabling does not follow the system recommendations, data loss might occur.

- Ethernet: CAT 5e or higher cable type:
  a. Minimum 30 cm. (0,98 ft.) and maximum 100m (328 ft.).

NOTE: The maximum length of 100 meters (328 feet) is only supported by the TIA/EIA 568-5-A standard that requires a 24 AWG wire diameter.

Ethernet cable testers

It is recommended to check the cables up front in order to ensure the functionality of the electronic connections. Therefore, cable testers are useful to verify connections are functional and if the transmission works prior to the installation.

Depending on switch brand and model, some switches may have the functionality of testing the Ethernet cable connectivity with the connected devices. This can be done using either a ping-functionality test or a TDR-test executed by the router or switch. Refer to the manufacturer of the network device for more information.

Fiber optics

There are two types of fiber –single or multi-mode- that may be used, depending on the distance of the cabling run. Single-mode fiber optic cable is best suitable for long distances due to its structure. In contrast, multi-mode fiber optic cable is most suitable for short or medium distances. Note, fiber optic cabling and infrastructure has to address impulse distortion and it is recommended to refer to the manufacturer of the fiber modules and cables for information about specifications and limitations. Distance and transmission rate may differ per manufacturer and model.

NOTE: Single mode connectors do not fit multi-mode modules and vice versa.

When purchasing a fiber optic cable, the orange colored cables are mainly designed for 1 and 2.7 Gbit/s connections, also known as OM2. The aqua colored cables are mainly designed for 10 Gbit/s connections, also known as OM3.

RTS Intercom devices that support fiber optic may be supplied with fiber modules. Please contact the RTS Intercoms sales representative, for more information.

OMNEO Suite

OMNEO Suite is delivered as a zip file which includes two folders. The OMNEO Suite is available for download from www.rtsintercoms.com. The .zip file contains the software applications and firmware files needed.

The folder named OMNEO Suite packages contains software installers for the computer including ARNI, AZedit, DNS-SD, FWUT, IPedit and USB drivers. All software applications included in this folder are compatible with the other software applications and firmware files included in the same OMNEO Suite.

The other folder included in the .zip file is the OMNEO Suite firmware which is used for updating OMNEO intercom devices. The updates are executed with the **FWUT** (Firmware Upload Tool) that is included in the OMNEO Suite as a separate installer. All firmware files included in the sub-folders are compatible with all other included firmware files. It is recommended to update all devices when performing an update at a single device in order to preserve compatibility between devices.

Domain Name System (DNS)

The **DNS** (Domain Name System) is a database in which all host names and corresponding IP addresses are stored. It is responsible for identifying and localizing IP-devices and resources on the internet and associating names with the corresponding IP address.

RTS Intercoms software applications make use of **DNS-SD** (DNS Service Discovery) for scanning neighbor devices in the same subnet for control or configuration purposes. The devices also make use of **mDNS** (Multicast DNS), as they are configured in order to connect to other devices based on the hostname(s).

If a device is no longer used operationally on the network, ensure the OMNEO device is removed from the configuration of the OMNEO-ports on the intercom matrix. This prevents unnecessary mDNS messaging over the network.

- Install the DNS-SD software included in the OMNEO Suite
- Remove OMNEO devices from the matrix port configuration as soon as it is no longer active

IP Addressing

An **IP** (Internet Protocol) address, is a unique address which identifies hardware over the network such as a computer, server, keypanel, interface cards or matrix. It allows a device to communicate with other devices over an IP-based network such as the LAN or WAN. There are multiple possibilities for assigning an IP-address to a device: DHCP, manual assignment and Link-Local.

Link-Local addresses are automatically assigned by the individual devices in cases where no static IP-addressing is assigned and a DHCP-server is not found. Addressing is based on the MAC-address of the device. Link-Local addressing can be recognized by an IP-address within the range of 169.254.0.0/16 (169.254.0.1 - 169.254.255.254) with 255.255.0.0 subnet mask. This Link-Local addressing is also known as APIPA-addressing. The Link-Local addressing scheme manages fixed IP-addresses in the same range as the devices automatically check availability of the IP-address, to ensure devices that do not support IPv4LL can operate in the same subnet.

DHCP (Dynamic Host Configuration Protocol) is a technology used to assign IP addresses and other related configuration information (such as subnet mask and default gateway) automatically to each device on a network. This is achieved by using a devices that contains a DCHP server, a feature frequently found in devices such as routers or an ARNI. The use of DHCP means IP addresses do not have to be assigned manually, thus providing reliable IP address configuration by minimizing errors. For smooth operation, the client and the DHCP-server must be in the same subnet to prevent communication and connection failures. When working in a critical environment, DHCP is the preferred method of setting up the network for the first time. However, with critical devices it is not recommended to use DHCP because IP-addressing might change over time and could produce unwanted results.

Manually assigned IP-addresses, also known as static or fixed IP-addressing, are only recommended if there is a good understanding of the network administration and assigned IP-addressing schemes already in place on the network. This is critical for preventing collisions and invalid or duplicate IP-addresses on the network. It is mandatory to enter a valid IP-address and subnet mask, while it is optional to enter a default gateway and DNS-server address. The default gateway is mandatory when data goes outside the **LAN** (Local Area Network) and the DNS-server is mandatory when an ARNI is used within the system. If there is a DHCP-server active, in addition to using fixed IP-addresses, it is recommended to exclude the fixed IP-addresses from the DHCP-address range.

Some devices can have multiple IP-addresses. This refers to devices that contain multiple **NIC** (Network Interface Cards) or with the protocols they are using. A good example is the **OMI** (OMNEO Interface) card which contains a controller and an audio IP-address.

- Two unique IP-addresses should be assigned to the OMI
  a. Controller IP-address
  b. Audio IP-address
- Managed switches requires an IP-address for configuration and routing features
- Private IP-address ranges are:
  a. 10.0.0.1 to 10.255.255.254 (16,777,216 addresses /8) with subnet 255.0.0.0
  b. 172.16.0.1 to 172.31.255.254 (1,048,576 addresses /12) with subnet 255.240.0.0
  c. 192.168.0.1 to 192.168.255.254 (65,536 addresses /16) with subnet 255.255.0.0

General requirements for OMNEO

Bandwidth

Bandwidth refers to the amount of data transmitted via the **LAN** (Local Area Network) and **WAN** (Wide Area Network) in a specific time period. It is usually measured in megabits per second (Mbps). Having higher bandwidth allows transmission of larger amounts of data and lower latency. To test the outbound connection, there are possibilities for doing a speed-test of the bandwidth.

On a LAN, it is common to have Gigabit Ethernet. Gigabit Ethernet transmits Ethernet packets at a rate of one gigabit per second and delivers low audio latency due to its fast connectivity.

- Each channel uses approximately of 2.9 Mbps bandwidth, but this may vary in each application and with each device
- It is mandatory to have Gigabit Ethernet connections between switches that interconnect the intercom devices

Managed switches

A managed switch provides capabilities to configure, manage and monitor the LAN. These functions result in greater control and security of data traffic and allows the prioritization of specific data flows. However, with the possibility of having more control over monitoring and security, also come great risks. Incorrect configurations of managed switches or routers can cause instability and communication problems can occur. The following items are required for a network is used with OMNEO equipment.

- A switch or router with the capability to forward more than 1,000,000 packets per second per port
- Support PIM-DM or bi-directional PIM
- Disable Energy Efficient Ethernet (EEE) or GreenEthernet

PIM-DM

PIM (Protocol Independent Multicast) is a collection of multicast routing protocols that provide one-to-many or many-to-many distribution of data by using routing information in the unicast routing table. This means that PIM is not dependant on any particular routing protocol for unicast traffic for its operation.

There are different variants of PIM including **DM** (Dense Mode) and the bidirectional PIM. PIM-DM assumes the multicast packet stream has receivers distributed densely throughout the network to receive the multicast feed. In order to execute the needed actions, PIM-DM builds shortest-path trees by flooding multicast traffic domain wide, and then pruning back branches of the tree where no receivers are present. If PIM-DM is not supported on the local network, it cannot forward traffic beyond its own subnet. It also indicates all other multicast traffic will not arrive either, which can lead to overloading the last reached router or managed switch with data. This can lead to slow or no activity.

In contrast, the bi-directional PIM, builds shared bi-directional trees. This means data flows in both directions along the branches. Therefore, its structure and functionality is designed to be used in “many-to-many” configurations.

EEE

EEE (Energy Efficient Ethernet) is a method to reduce power consumption while using an Ethernet device during periods of low or no data activity. On some switch models, this is called GreenEthernet, but has the same effect.

Even if EEE is useful for potential power saving on the network, it affects the intercom system negatively when trying to save power on ports used by intercom devices. Ports become inactive while the intercom device sends out data. Because the port is inactive, the device may seem unresponsive. Once the switch has collected enough data for the device to become active, the switch port the devices are connected to receives connectivity again. Due to this delay, packages arrive with delay, including **PTP** (Precision Time Protocol) packets. This causes audio mutes or glitches. In critical environments with intercom communication, the risk of losing connection is high, so it is recommended to deactivate this feature in the switch. If the switch cannot deactivate this feature, it is not suitable for intercoms. Note, some unmanaged switches implement this feature without the possibility to disable it.

- Disable EEE or GreenEthernet

VLAN

VLAN (Virtual Local Area Networks) provide a logical segmentation of networks for separating traffic. VLANs allow one LAN to work virtually as multiple networks by having multiple networks connected to the same physical infrastructure. Packets are only forwarded to another network when needed. A router, or a specialized Layer 3 switch, connects VLANs to each other since each VLAN has a different subnet. This method ensures security and flexibility, but at the same time might limit communication between devices in the network. This feature can be configured on many managed switches or routers and requires a good, in depth, understanding before applying.

- All OMNEO devices in the same VLAN;
- Preferred all OMNEO device in the management VLAN.
  a. For Cisco devices, VLAN 1 is the management VLAN w/o restrictions.

LLDP

The **LLDP** (Link Layer Discovery Protocol) is a vendor-neutral configuration exchange protocol for layer 2 discovery based on the IEEE 802.1ab standard. This protocol allows devices to advertise information such as its identity or capabilities to its neighbor. The receiving device stores the information gathered in the device as a **MIB** (Management Information Base). Even when static IP-addressing or DHCP is used, LLDP still provides the profitability of discovering devices for software, service and device applications.

- Enable LLDP

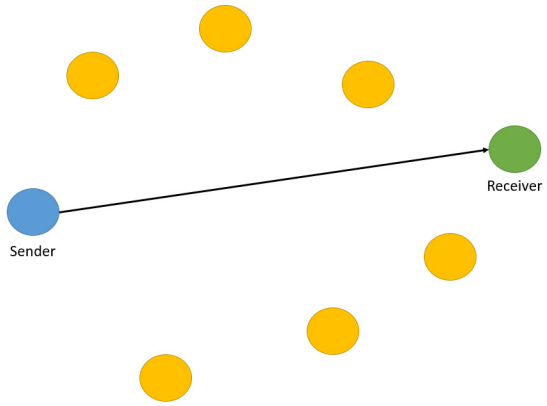
IGMP

IGMP (Internet Group Management Protocol) is the communication protocol responsible for communication between the end devices (hosts) and the switch or router. It is used for dynamic multicasting, which can be the communication type between one source and a selected group of destinations by establishing multicast group memberships. For this purpose, IGMP can register a router to join and to allow specific groups to receive or not receive specific multicast traffic. The process of monitoring this IGMP traffic between hosts and router is called IGMP snooping. The information gathered is used to map the links to the specific interfaces based on their group membership. This means IP multicast streams are only forwarded to interfaces connected to the hosts that want to receive it.

- Disable IGMP snooping at the OMNEO network

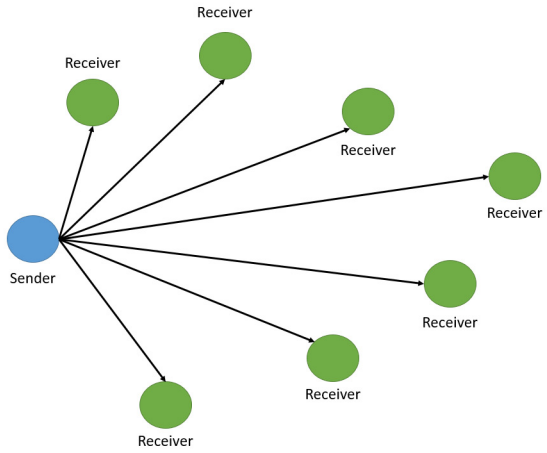
Unicast

Unicast is used for one-to-one, also known as point-to-point, transmission with one (1) sender and one (1) receiver. A switch detects which port a unicast IP-address is connected to and only forward packets to this port.



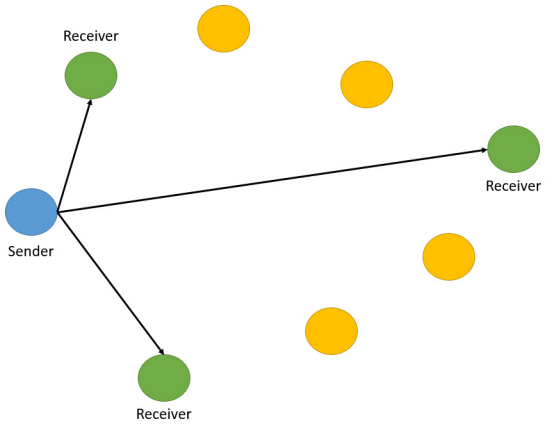
Broadcast

Broadcast is used for one-to-all transmission with one (1) sender and multiple receivers. With broadcast, the packets are sent to all devices in the subnet or VLAN. The data is then processed by the devices that need it, but ignored by others that do not. However, the bandwidth on the link is still utilized by sending this information.



Multicast

Multicast is used for one-to-many transmission with just one (1) sender and multiple receivers. Multicast differs from broadcast in that packets are sent only to the devices and ports that are interested in the data. This means that multicast traffic can make much more efficient use of available network bandwidth, but may also require the use of IGMP for management.



RSTP

The **RSTP** (Rapid Spanning-Tree Protocol), also as a standardized 802.1D-2004, is an evolution of the **STP** (Spanning Tree Protocol). The primary goal of RSTP is to use redundant network connectivity without causing network loops. With the RSTP protocol each device can calculate the shortest path to the RSTP root switch and only use this path to communicate to other networked devices. As soon as a connection fails, a new path is calculated within seconds and communication continues. This is also known as switched redundancy by DANTE controller. For RTS Intercom devices that use RTSP methodology, it is important this is enabled via IPedit at each device.

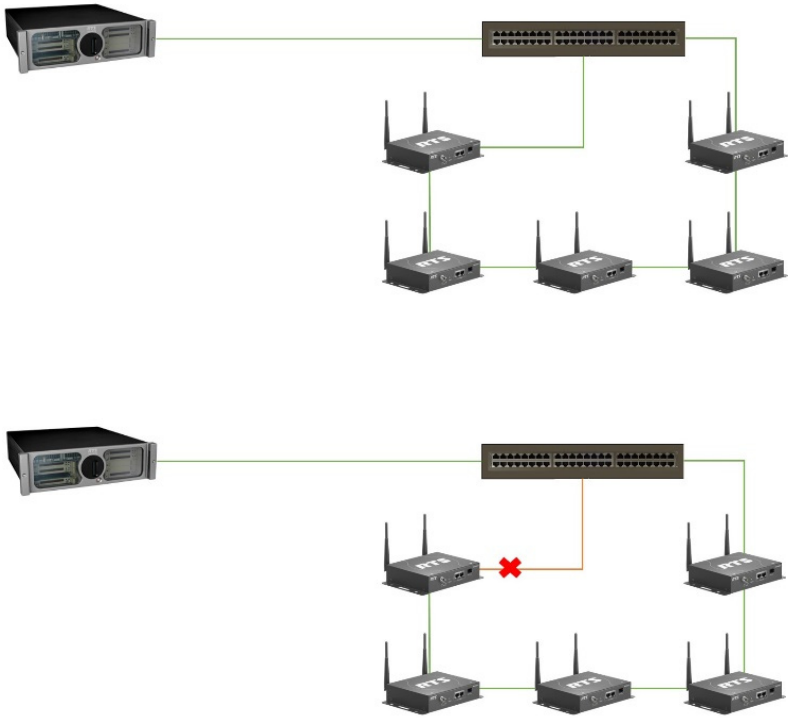
To achieve the goal of RSTP, it utilizes **BPDU** (Bridge Protocol Data Units). BPDUs are used for exchanging configuration messages across switches within an extended LAN using the RSTP topology. BPDUs are frames containing information about ports, switches and addresses which is sent out on a consistent basis of nine seconds. BPDU messaging might be seen as a threat when the switches or routers do not allow this type of messaging on edge-ports, which might result into blocked network ports or switches and routers turning into inactive mode. It is important to allow these types of messages.

- All switches and/or routers compatibility with IEEE802. 1D-2004 (RSTP)
- Firmware loaded on the OMNEO devices with support of IEEE802. 1D-2004 (RSTP)
- Allow BPDU messaging on the network ports with OMNEO devices (edge ports)
- Maximum 21 hops excluding the root bridge when using RSTP
- Route bridge priority works with values, where a low value is equal to high priority in the network
- Required bridge RSTP settings:
    a. Hello time of 9 seconds
    b. Maximum age of 22 seconds
    c. Forward delay of 30 seconds

Daisy chain

A daisy chain is a series of devices connected to each other in order to have connectivity to the main network. In a daisy chain, each device is counted as a hop. Devices can have limitations on the maximum amount of hops allowed between them. It is recommended to have up to 21 devices interconnected in a daisy chain, either in a linear or ring topology.

- Maximum 21 devices in a daisy chain as these count as a hop.



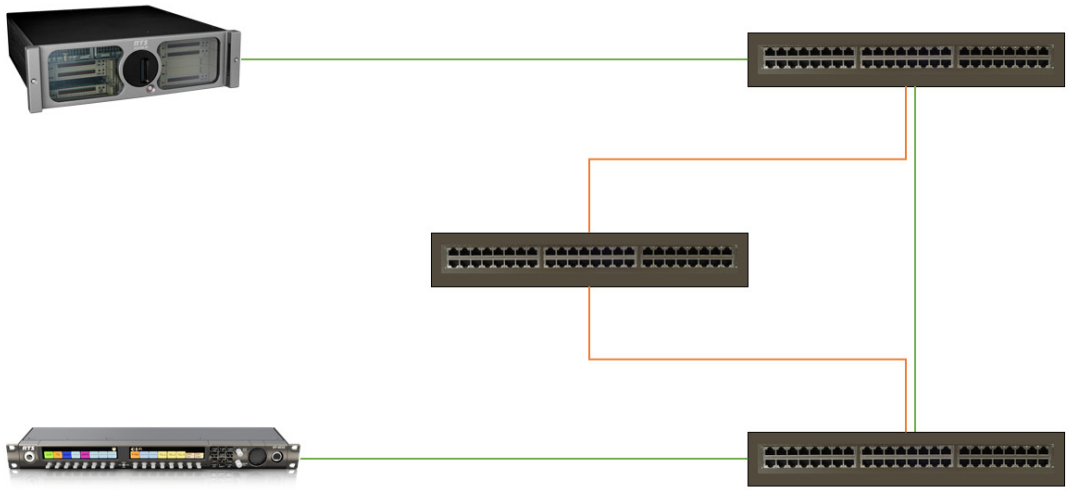
In this example, the devices are interconnected as a daisy chain loop. A daisy chain loop is easy and fast to install and can be used as an ad-hoc solution. In case of cable or device failure between devices, the communication path continues via the other end. If the device contains an Ethernet port(s) and fiber optic port(s) both marked as OMNEO, a combination of Ethernet and fiber can be used to extend the distance between the switch or router and first connected devices of the chain.

NOTE:

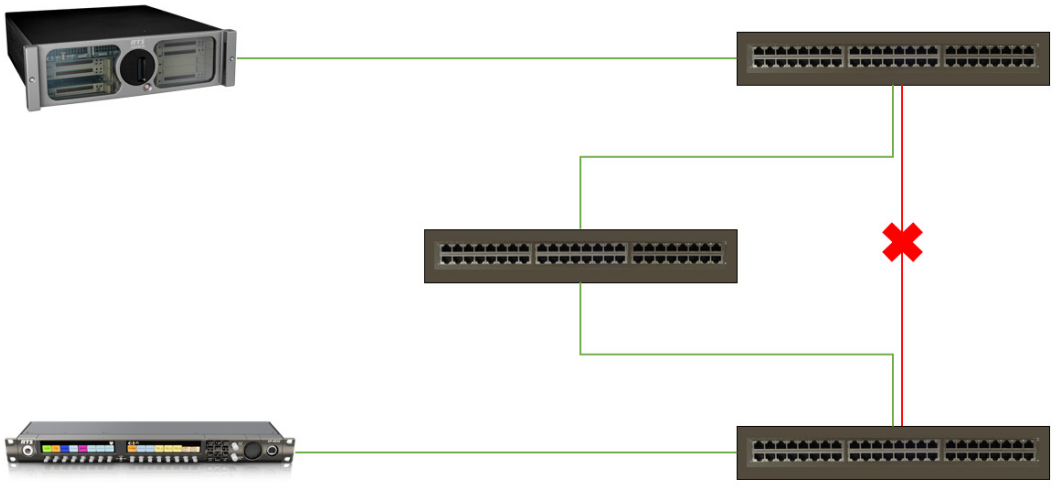
- This is only recommended as ad-hoc or temporary solution.
- This solution requires Rapid Spanning-Tree Protocol (RSTP) being enabled at the switch or router.
- The devices require Rapid Spanning-Tree Protocol (RSTP) firmware being loaded.

Rapid Spanning-Tree Protocol in drawing

In this example, there are two routes between the switches. From the top switch to the lower switch, there is a direct connection and a back-up connection via a switch in between. The fastest connection is the main route and it has to do with the connection speed rather than the number of devices in between.

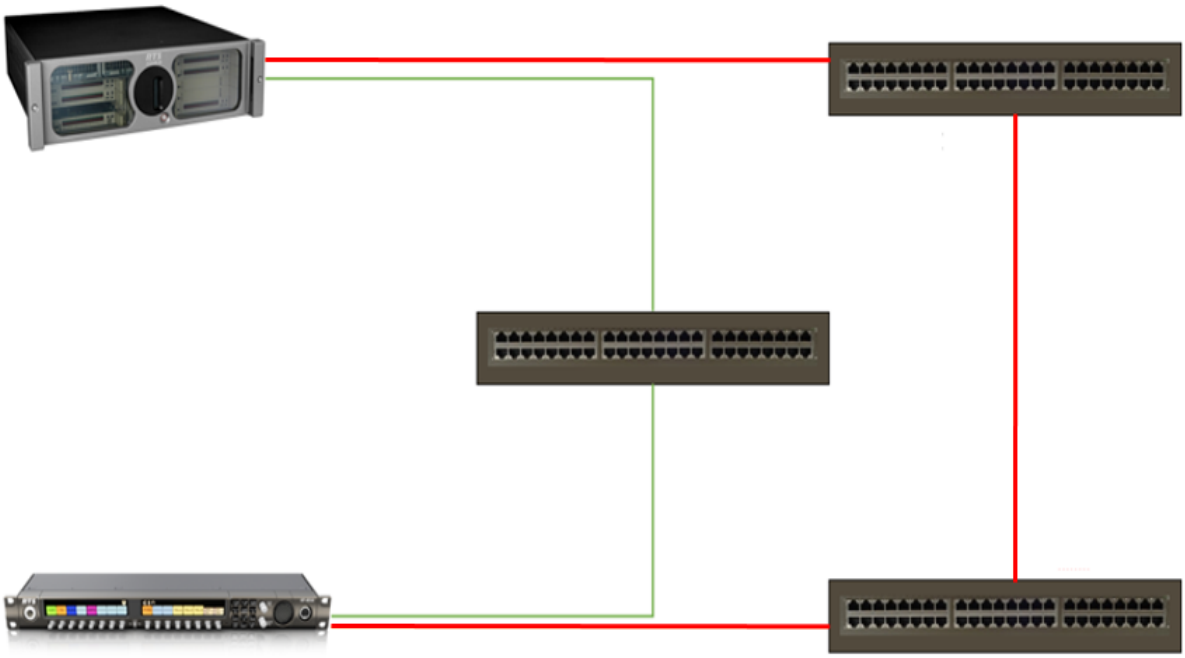


In this example, the direct connection between two switches has failed. As RSTP is active, the routes are known and another route is taken for communication between the devices. Also, there is only one back-up connection, but with RSTP there can be multiple routes available not just one or two.



In this example, the ADAM M matrix has two connection by OMI interface to two different switches. The end-device, a keypanel single rack unit. uses OMNEO connected to two different switches. As well, the OMI as the keypanel can have only one Ethernet link active, with the second Ethernet link standby, the fastest route is used in order to reach the destination from the source. Between the switches, network information is shared about active links and end-devices. When one of the connections fails, the audio and data transmission switches over to secondary route.

NOTE: For more information on RSTP deployment, contact RTS technical support.

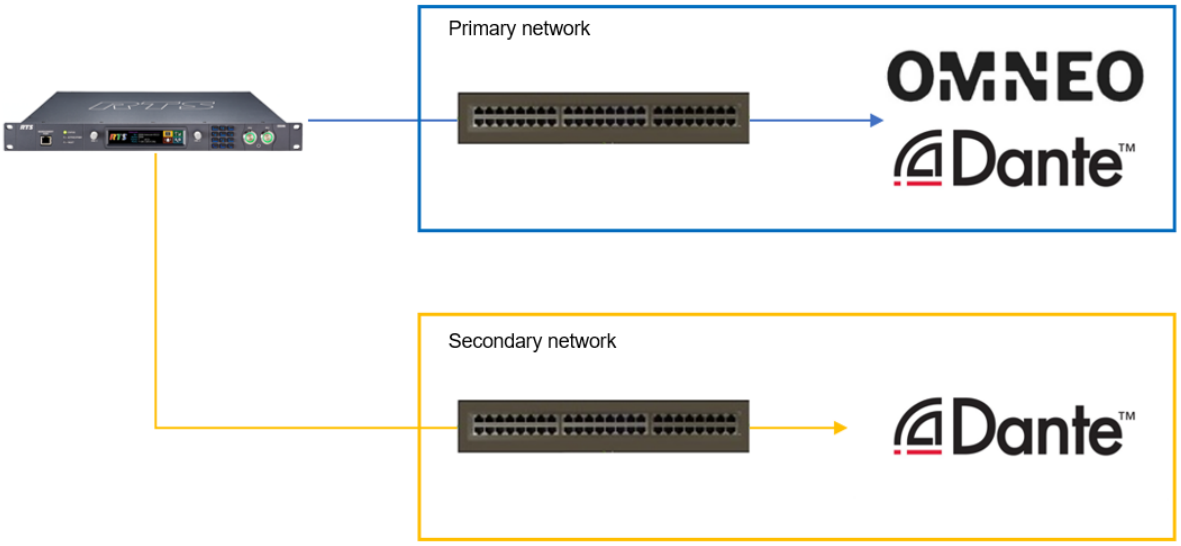


Glitch-free

Glitch-free, similar to the standard ST 2022-7, is known as two different Ethernet or Fiber optic ports of one device connected to two different network environments in which both Ethernet or Fiber optic ports are active at the same time. In other words, one device is able to communicate to two different network environments. The data has the same destination and therefore the audio that arrives twice at the destination. This way we can guarantee that audio and data always reaching the destination by using different routes in the network. In DANTE controller this is named as redundant. It is possible to combine DANTE glitch-free redundancy with OMNEO RSTP. Glitch-free is redundancy by the end-device rather than from the network infrastructure. Note, even when RSTP and Glitch-free can be functional at the same network, RSTP can only be active at the primary network as it only has one active Ethernet link where glitch free can be active at primary and secondary network by having two active Ethernet links at the same time. In other words, a device that supports glitch free, such as ODIN, requires to use a source and destination for each audio channel which has to go to DANTE device in glitch free redundancy mode. For more information about RSTP, see Figure , “RSTP,” on page 9.

Glitch-free can be enabled in IPedit and DANTE controller, however the second Ethernet or Fiber optic port IP addressing can only be set via DANTE controller. The second IP Address is only capable of sending audio. After enabling Glitch-free mode the device resets and is not available for operation during its boot process.

NOTE: When deploying glitch free and RSTP in the same network, ensure the switches and routers are not linked together in any sense as RSTP prevents network loops.



QoS)

QoS (Quality of Service) is a set of technologies that manages network traffic based on settings or traffic behavior. It prioritizes traffic on the network based on the type of protocol by providing differentiated handling and capacity allocation to specific flows of network traffic. QoS is provided by **DiffServ** (Differentiated Services) which is a type of traffic management. It uses a 6-bit code, also known as the **DSCP** (Differentiated Services Code Point), in order to classify the IP packets. Forwarding behavior, also known as per hop behavior, is assigned to each packet transmitted though the network. This determines how IP packet data is forwarded. If you do not have experience with QoS or DiffServ, and if no external traffic is present on the network, it is recommended to leave all settings at their default values within the managed switch. Only managed switches have QoS functionality.

OMNEO uses QoS with DiffServ to ensure synchronization of the audio devices works accurately. This is especially needed for networks with a relatively high bandwidth usage (>20%). Please refer to the manuals of the IP-infrastructure devices first before applying QoS.

- Mandatory DSCP values set for prioritization of packages:
  a. DSCP-PTP time sync and delay request events highest priority
     - DSCP value 56 decimal, 0x38 hexadecimal
     - DSCP label CS7
  a. Audio, PTP time sync follow-up and delay response set to high priority
     - DSCP value 46 decimal, 0x2E hexadecimal
     - DSCP label EF
  a. Reservation of medium priority
     - DSCP value 8 decimal, 0x08 hexadecimal
     - DSCP label CS1
  a. Other traffic set to low priority
     - DSCP value 0 decimal, 0x00 hexadecimal
     - DSCP label CS0

SNMP

SNNP (Simple Network Management Protocol), a component of a larger software package, is used for monitoring hardware and software. SNMP is used in larger networks to communicate with the devices in the network and most importantly gather information from them, such as errors.

OMNEO devices make use of SNMP version 1. SNMP version 1 is supported by most SNMP monitoring software.

MIB

A **MIB** (Management Information Base) is a database used for managing the entities in an IP-infrastructure. The database is hierarchical (tree-structure) and each entry is addressed through an **OID** (Object Identifier). Each OID refers to a different component or service, which is sent out as a TRAP message, in case of failure or warning. The OID is translated by the SNMP monitor into clear text to ensure the operator is aware the message is received and can take appropriate action.

Each device has its own MIB-file required for SNMP monitoring. Devices that use the same software and have similar hardware, usually have the same MIB-file.

Trap messaging

A trap is a type of error or warning caused by exceptional conditions. A trap in a system process is more serious than a trap in a user process. Traps in a system process are more serious because they may signal spikes in operating temperatures, invalid memory or software. Any Trap message is an alarm or report about the managed subsystem.

Port management

UDP (User Datagram Protocols) and **TCP** (Transmission Control Protocols) are the major transport protocols for sending packets over the internet. TCP confirms the receipt of the packets and retransmits any lost packets. Additionally, it guarantees an error-free transaction because of its a tracking feature. TCP is more reliable than UDP because of error checking and receipt acknowledgement capabilities. However, this also means that TCP packets require additional time for queueing, processing, and acknowledgement. UDP does not have these additional features, but is much faster and more efficient. It is typically used for data such as real-time audio, as lost packets are relatively rare in a properly designed network. OMNEO uses UDP for audio transmission and TCP for control data transmission.

Port	Protocol	Description
69	UDP	OMNEO firmware downloads (TFTP)
161-162	UDP	SNMP listen and TRAPs
319 - 320	UDP	PTP clocking
2076	UDP	RVON VoIP signaling
2077	UDP	RVON VoIP audio
2079	UDP	RVON call request or permission
2080	TCP	OMNEO keypanel data
2081 - 2082	UDP	Pass-through serial port 1 and 2
2082	TCP	AZedit firmware downloads
2100	TCP and UDP	IPedit remote administration
2100	UDP	IPedit send and receive
2200	UDP	Proprietary messaging / offer port
4321	UDP	DANTE audio
4440 - 4455	UDP	DANTE routing
5004	UDP	AES67 streaming
5353	UDP	Multicast DNS
8000	TCP	OMNEO keypanel data
8700 - 8800	UDP	DANTE control and monitoring
9470	TCP	OCP discovery and registration
9471	TCP	OCP TLS listening
9472	UDP	OCP periodic controller events
9473	UDP	OCP reset events
9474	TCP or UDP	ARNI unicast communication
27409	UDP	TM-2000 active and standby messaging
27410 - 27411	UDP	TrunkEdit data transmission and discovery
27410 - 27411	UDP	AZedit data transmission and discovery
27412	UDP	AZedit GPIO configuration
27413 - 27414	UDP	MCII-e and GPIO communication
27415	UDP	MCII-e multi-frame communication
27415	UDP	TM-2000 trunking data
14336 - 14600	UDP	DANTE audio communication
49152 - 65535	TCP	OCA firmware
49152 - 65535	TCP	OCA insecure services w/ dynamic port selection
49152 - 65535	TCP	OCA secure services w/ dynamic port selection

Appendix - OMNEO or RVON

OMNEO supports private network environments with a maximum latency of 20ms and a minimum of 2,05 Mbps bandwidth. In network environments that fulfill these requirements, all OMNEO keypanels (OKP) or other OMNEO devices (OMI, OKI, OEI and OAP) are able to communicate. These devices or interfaces require OMNEO firmware, which can be found in one of the OMNEO Suites.

These OMNEO compatible devices support fixed, DHCP and Link-local IP-addressing. In large systems with more than 128 OMNEO devices, an ARNI is required to handle clocking and DNS.

RVON (RTS Voice Over Network) supports external communication with a longer latency and can go across networks. When using RVON, the communication devices require RVON firmware to be compatible and can only communicate to a RVON interface card in the matrix. Note, there are two modes: local and remote mode.

Local mode is used for local keypanels directly connected to a matrix. Remote mode is used for digital keypanels connected with RVON expansions going through WAN connectivity before connecting to a matrix. Additionally, remote mode is used for trunking. These modes can be set via a DIP switch.

It is recommended to have one LAN or VLAN designed for OMNEO, one LAN or VLAN for RVON, and one LAN or VLAN for DANTE devices. This makes troubleshooting easy and avoids traffic interference between the different protocols.

Appendix - Precision Time Protocol

PTP (Precision Time Protocol), specified in IEEE 1588, is a packet-based technology used to synchronize the media clocks of all OMNEO devices. In order to achieve the time synchronization, packets are transmitted and received between a master clock and a slave clock. The master clock is selected automatically or provided by a specific device (e.g. ARNI, PTP grandmaster). All other devices operate in PTP slave mode and synchronize to the master. The network latency between the master and the slaves is measured and compensated so all devices run synchronously. There are two versions. PTP version 1 is adjusted to measurement applications and industrial machines. The second version, called PTPv2, poses an extension of version 1. It is based on Ethernet and not backwards compatible.

- When OMNEO is speaking Dante natively, it will use PTPv1, like all other Dante devices
- If AES67 is used, a PTPv2 boundary clock will be created and synchronized to the other PTPv1 devices

Please contact technical support for more information about AES67 and bridging PTP version 1 and version 2 on your network.

Appendix – ARNI

The **ARNI** (Audio Routed Network Interface) is a hardware device that enhances the scalability of the OMNEO system. There are two types of ARNI-modes.

ARNI-S (ARNI-Standard) supports up to 450 OMNEO nodes in a signal subnet. It can act as a DHCP-server DNS-server, and is the PTP clock master for its own network.

ARNI-E (ARNI-Enterprise) supports up to 10,000 OMNEO nodes in multiple subnets (up to 40 subnets) and is used in parallel with an ARNI-S. By itself, ARNI-E can also support up to 450 OMNEO nodes. ARNI-E acts as a clock master for the entire system, where all ARNI-S devices follows the enterprise and synchronize the clock in each subnet.

By acting as a DHCP-server, the ARNI eliminates the use of IPv4LL protocol and supports one subnet in case there is no other DHCP server yet.

By acting as a DNS-server, it stores all records of nodes and responding to controller queries and resolve hostnames. ARNI uses DNS-SD (Service Directory) protocol to store and scan devices.

By extending the PTP clocking over multiple IP-subnets, it can act as a boundary clock, synchronized to a master clock using unicast PTP-messaging and acting as a clock master in its own subnet by using multicast PTP-messaging to synchronize the OMNEO nodes. All OMNEO devices operate at PTP version 1.

NOTE: For more information, see the ARNI technical manual.

Appendix – TTL

TTL (Time To Live) is a mechanism that limits the lifetime of data p0ackages in an IP-infrastructure. When data is passed through routers, the TTL is decreased by 1. In case TTL has reached 0 and the data has not reached its destination yet, the data is discarded. This setting prevents that data passing through indefinitely in a network and improves the performance4 of the IP-infrastructure overall by preventing unnecessary cache use at switches and routers. The maximum value of TTL is 255, however, it is recommended to initially set TTL at 128.

NOTE: TTL is only valid when routers are deployed and communication is meant for another network.

Bosch Security Systems, Inc.
12000 Portland Avenue South
Burnsville, MN 55337 U.S.A.
www.boschcommunications.com