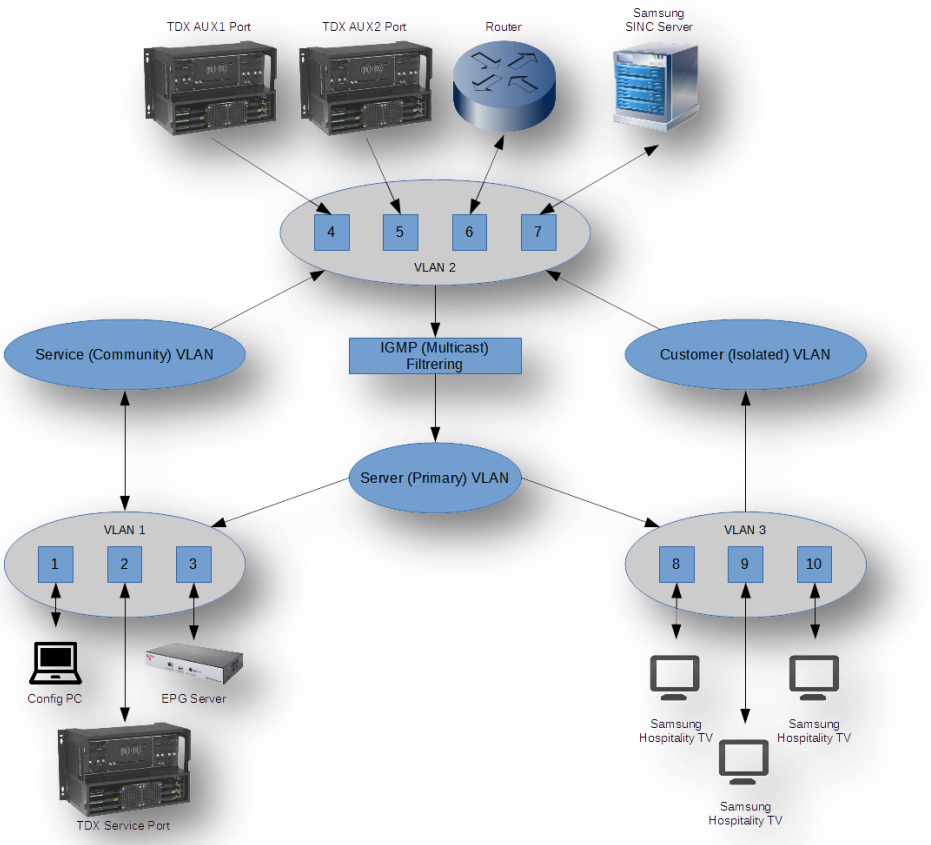
TRIAX
connecting the future



Installation Guide

TRIAX Switch setup for Hospitality systems

Article	Article no.
TRIAX Switch setup for Hospitality systems	

Version	891089A	Date	07/2016	EN

triax.com

Table of contents / Inhaltsverzeichnis / Sommaire

1. Scope

This paper is meant to describe the setup principles associated with running a Samsung SINC Server Hospitality system with the TDX Headend. It deals with some issues that are specific to the TDX and the Samsung SINC server, but this information may be applicable to other systems as well. The document will not contain a step-by-step guide to setting up a switch for a hotel, as the variations in switches and number of ports and topography is simply too varied to make an effective guide. The reader should, however, be able to set up any switch after reading this document, with minimal effort.

2. Concept description

2.1 System overview

A TDX Headend setup with the Samsung SINC server is an IPTV based Hospitality solution. The model in Fig. 1 shows a theoretical representation of a hotel, where each floor has a separate router, each wired to a main router in the basement

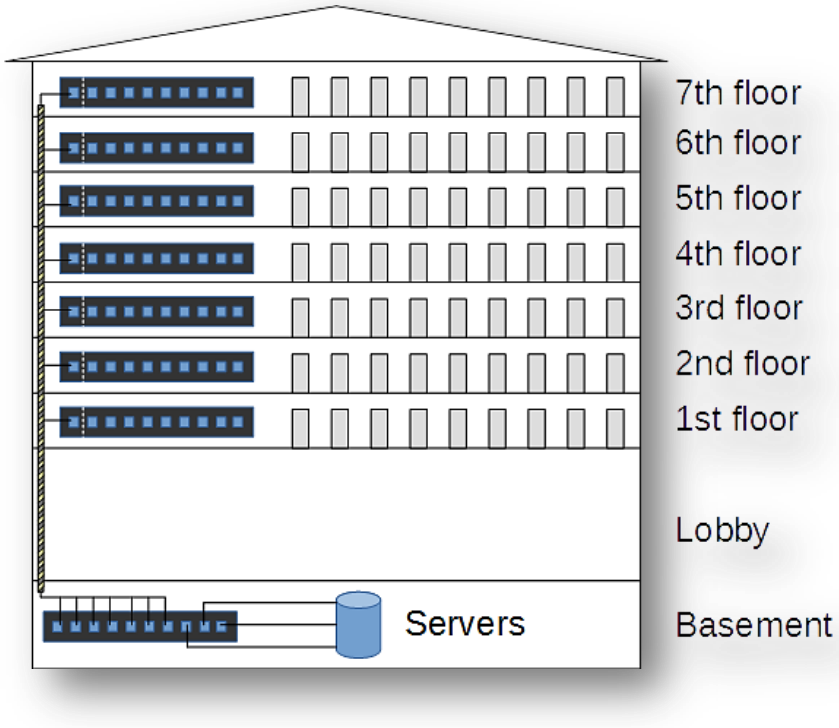


Fig. 1

2.2 Wiring typography

Background knowledge

Since the IPTV services are multicast, the main switch will copy the transport stream packages belonging to a particular service to any port that requests to be a member of that multicast service (this requires that the switch is set up in a particular fashion). This setup is designed to limit the data on the Ethernet connection, as users don't need to request a specific package. Thereby it limits the need for switching in the router, since it will just copy the data from the ingress (incoming) port to the egress (outgoing) port. This means that a switch can copy 700 Mbit/s of incoming multicast data to each of its other Ethernet ports.

2.3 Serial – Bus – Star configuration

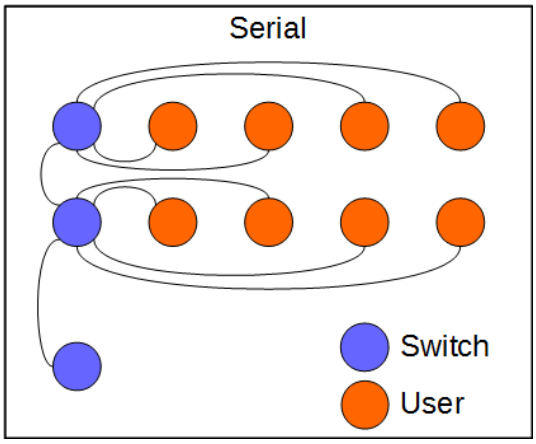


Fig. 2 Serial configuration

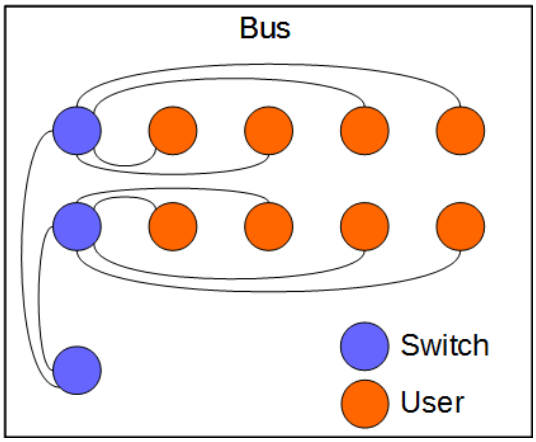


Fig. 3 Bus configuration

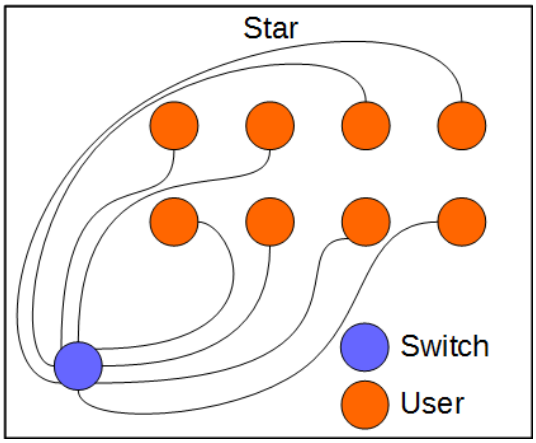


Fig. 4 Star configuration

Serial configuration
The Serial configuration, sketched in Figure 2 connects the 1st floor router to the 2nd floor router and the 2nd floor router to the 3rd floor router and so on.
If we calculate the available IPTV bandwidth, based on the theoretical hotel in Figure 1, there are 63 users for about 700Mbit/s bandwidth (the maximum output-bandwidth the TDX can deliver), because all users are connected to one port on the main switch. This results in about 11Mbit/s per user, and is well within the range of a HDTV service. This means that the users would struggle to watch 63 different HDTV services at the same time.
Bus configuration
This configuration, sketched in Figure 3 is more wire-heavy than a Serial configuration, but less wire heavy than a Star configuration (see below). The Bus configuration ensures that each floor has a direct connection to the main switch, resulting in a full 1Gbit connection available to each switch on every floor.
This means that in the theoretical hotel in Figure 1, each room would have about 78Mbit/s available, which is plenty.
Star configuration
Star configuration, sketched in Figure 4, connects wiring between each room directly to the basement. This would provide a full 700Mbit/s connection to each room. The solution requires a lot of cabling and is not very practical, not to mention the fact that the available bandwidth is unnecessary in a hotel

2.4 The core issue

The issue with the IPTV Hospitality solution is that the IPTV streaming output, the EPG Server, the Samsung SINC server, the internet router and the TDX Service Port is on the same switch as the users. Therefore there is a potential risk that a user may hack the TDX and change his TV privileges or sabotage the stream altogether. Additionally there is a risk of one user (hotel guest), hacking another.

3. Requirements

3.1 Multicast filtering

When transmitting IPTV Services, the Transport Stream is sent as multicast frames. These multicast frames are normally received by one port in the switch, copied and transmitted by all the other ports. This results in a lot of unnecessary data on the ports, especially when you have two ports with potentially 700Mbit/s of transport stream data.

The answer to this problem is to filter the multicast data, so the data will only be sent out on the ports that actually ask to be part of that particular stream. To achieve this, a managed switch can be set up to filter the multicast frames based upon membership tables held by the IGMP network Querier.

3.2 Isolation

We need to have a system that separates the TDX Management port from the users.
However, the Users must be able to access the SINC server, the Streaming outputs and the Router in order for the Smart TVs to work.
Lastly, the EPG server should have access to the TDX Management port for future use and the SINC server must be able to access the EPG Server in order to fetch the EPG data XML file.
The connections can be put into a matrix:

TRAFFIC → INCOMING	Admin port	TDX Service port	EPG Server	TDX AUX port 1	TDX AUX port 2	Samsung SINC Server	Internet Router	User/Guest 1	User/Guest 2	User/Guest n
Admin port	+	+	+	+	+	+	+	-	-	-
TDX Service port	+	+	+	-	-	-	-	-	-	-
EPG Server	+	+	+	+	+	+	-	-	-	-
TDX AUX port 1	-	-	-	+	-	-	-	-	-	-
TDX AUX port 2	-	-	-	-	+	-	-	-	-	-
Samsung SINC Server	+	-	+	-	-	+	+	+	+	+
Internet Router	+	-	-	-	-	+	+	+	+	+
User/Guest 1	-	-	-	+	+	+	+	+	-	-
User/Guest 2	-	-	-	+	+	+	+	-	+	-
User/Guest n	-	-	-	+	+	+	+	-	-	+

Table 1: Asymmetrical connection matrix for isolation of users

	Admin port	TDX Service port	EPG Server	TDX AUX port 1	TDX AUX port 2	Samsung SINC Server	Internet Router	User/Guest 1	User/Guest 2	User/Guest n
	INCOMING TRAFFIC →									
Admin port	+	+	+	+	+	+	+	-	-	-
TDX Service port	+	+	+	+	+	+	+	-	-	-
EPG Server	+	+	+	+	+	+	+	-	-	-
TDX AUX port 1	+	+	+	+	+	+	+	+	+	+
TDX AUX port 2	+	+	+	+	+	+	+	+	+	+
Samsung SINC Server	+	+	+	+	+	+	+	+	+	+
Internet Router	+	+	+	+	+	+	+	+	+	+
User/Guest 1	-	-	-	+	+	+	+	+	-	-
User/Guest 2	-	-	-	+	+	+	+	-	+	-
User/Guest n	-	-	-	+	+	+	+	-	-	+

Table 2: Symmetrical connection matrix for isolation of users

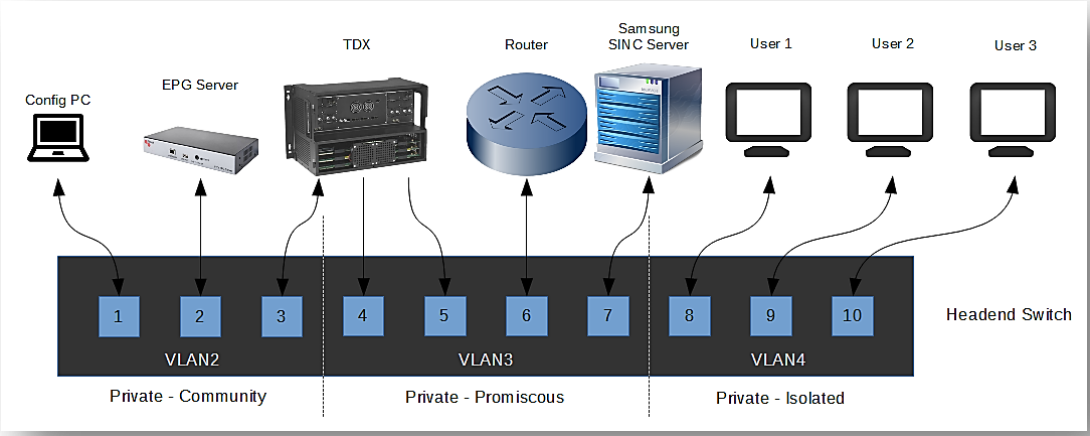
3.3 Implementation

This principle can be implemented in a number of switches. What follows is a description of the switches we have successfully programmed in this way.

Cisco SG300-10/SG300-20
To program the cisco switch for multicast filtering, the admin needs to globally enable the multicast filtering, then they need to enable unregistered multicast filtering on each of the physical ports. Then the admin needs to enable IGMP snooping and connect the snooping functionality to the VLAN that all the users have access to. Finally the IGMP snooping function must be set to immediate-leave to prevent old connections from being a problem when creating new ones and set the switch as IGMP Query (see section 3.1).

When the multicast filtering is done, a number of VLANs are set up to isolate the users/guests from the management network. On the Cisco switch, 3 Private VLANs are set:

- VLAN 1: This is the default VLAN. This cannot be erased or given advanced functions
- VLAN 2: This is the Service VLAN. It is used to access the servers by the service technician and contains ports from the TDX and EGP Server that should not be accessible by the users/guests.
- VLAN 3: This is the Server VLAN. This is used for the servers and routers that should be visible to both the service technician and the users/guests.
- VLAN 4: This is the User VLAN: This is where the users/guests are connected to the switch. The extra feature here is that not only should these users not be able to connect to ports connected to the Service VLAN, but also should not be able to connect to other users. Therefore this VLAN is designated as "Isolated"



The physical ports are then associated with the VLANs the devices connected to them should belong to, according to Table 2.. The left side of Table 2. is connected to VLAN 2 (Service), the middle is assigned to VLAN 3 (Servers) and the right side is connected to VLAN 4 (Users).
The way this works in the Cisco switch is that the primary VLAN is VLAN 3, which can connect to all ports. The ports belonging to the Service group then have VLAN 2 as its secondary VLAN and the ports belonging to the User group have VLAN 4 as its secondary VLAN. The ports only associated with the Server group are set as "Promiscuous" to allow all VLANs to communicate with it.
This means the servers can communicate with everyone, the Service devices can communicate with the other Service devices and the Servers and the Users can communicate with the Servers only.
A configuration file is available on http://www.triax.com/Support.aspx.

ZyXEL XGS-4526
Multicast filtering and snooping is set under in the Multicast>Multicast Setting menu. Here it is important to set up a filtering profile that covers all the IP addresses that are used by the TDX to broadcast IPTV streams. When that is done, the profile can be applied to all ports and all ports can be set to immediately leave the streams when done watching.

The ZyXEL Switch is somewhat easier to set up when it comes to the VLANs. When the Switch Setup is set to "Port based" VLANs, the VLAN setup page will display a connection matrix, much like the one displayed in Table 1 and table 2.. Here you can control which ports data from a specific ingress port is able to reach.

Stackability
When setting up a hotel, you will usually have multiple switches, in the case of our hotel model in Fig. 1; we have one head switch which is connected to the TDX headend and one sub-switch for each floor. If the head switch is set up in the fashion described in 0 or 0, the sub switches can be set up with a secondary, isolated VLAN, covering ports 2 to 10 and a primary promiscuous VLAN covering port 1. This will make port 1 an "Uplink" to the head switch.
The multicast filtering is set up in the same way as in the head switch, with the exception that there can only be one query in each network, so this function should be disabled in the sub-switches.

4. Conclusion

Setting up a switch with the functions we require to use IPTV Backend is relatively easy when you understand the theory behind the setup.

1) There needs to be an IGMP filtering in effect to avoid overloading the switch with data.
2) There needs to be an isolation of the users from the Service ports, in order for the system to be secure.

It should be noted that as long as the Users does not have to access the service ports directly, this system is relatively secure, but since some TVs require information, only available on restricted ports, this setup cannot be used in all circumstances.

TRIAX
connecting the future

For further information
and updated manuals go to

triax.com/support

TRIAX A/S | Bjørnkærvej 3 | Hornsyld | Denmark

triax.com