INTERACTION INSIGHT CORPORATION
GETTING YOU CLOSER TO YOUR CUSTOMERS

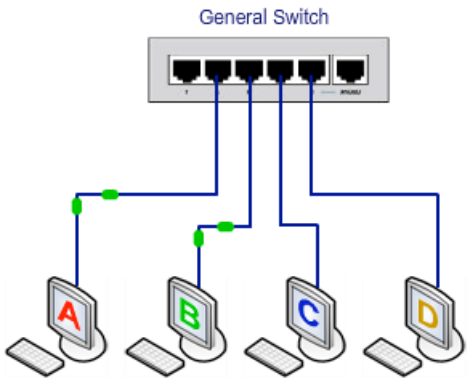
PORT MIRRORING OVERVIEW

Port Mirroring, also known as **SPAN (Switched Port Analyzer)**, is a method of monitoring network traffic. With port mirroring enabled, the switch sends a copy of all network packets seen on one port (or an entire VLAN) to another port, where the packet can be analyzed.

Port Mirroring function is supported by almost all enterprise-class switches (managed switches).

Port mirroring function is best described when comparing regular switch and switch with port mirroring support.

Figure 1. Regular Switch



In Figure 1 you see network the traffic sent between computers A and B.

The MAC table in the memory of the switch contains information on which port is connected to which computer.

Switch knows that:

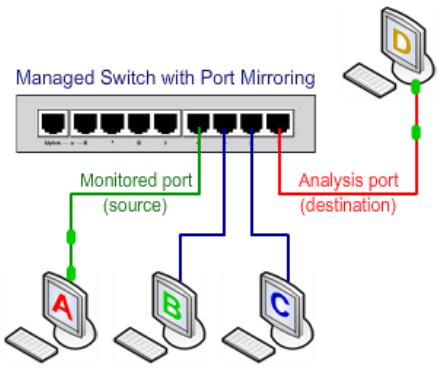
- Port #1 (first on the left) is not connected.
- Port #2 is connected to A
- Port #3 is connected to B
- Port #4 is connected to C
- Port #5 is connected to D

When the switch receives a packet from A to B, it routers this packet to port #3 (because B is on port #3).

Other computers (C and D) do not see this network traffic. It is hidden from them.

Conclusion: With a regular switch the network traffic is visible only to computers, which directly participate in a communication. Other computers do not see the traffic, which is not destined for them.

Figure 2. Switch with Port Mirroring



In Figure 2 you see the similar scenario: the network traffic is sent between computers A and B.

But there is a small difference: this switch supports port mirroring function. And administrator has configured the switch to mirror to computer D all network packets, which are transmitted between computers A and B.

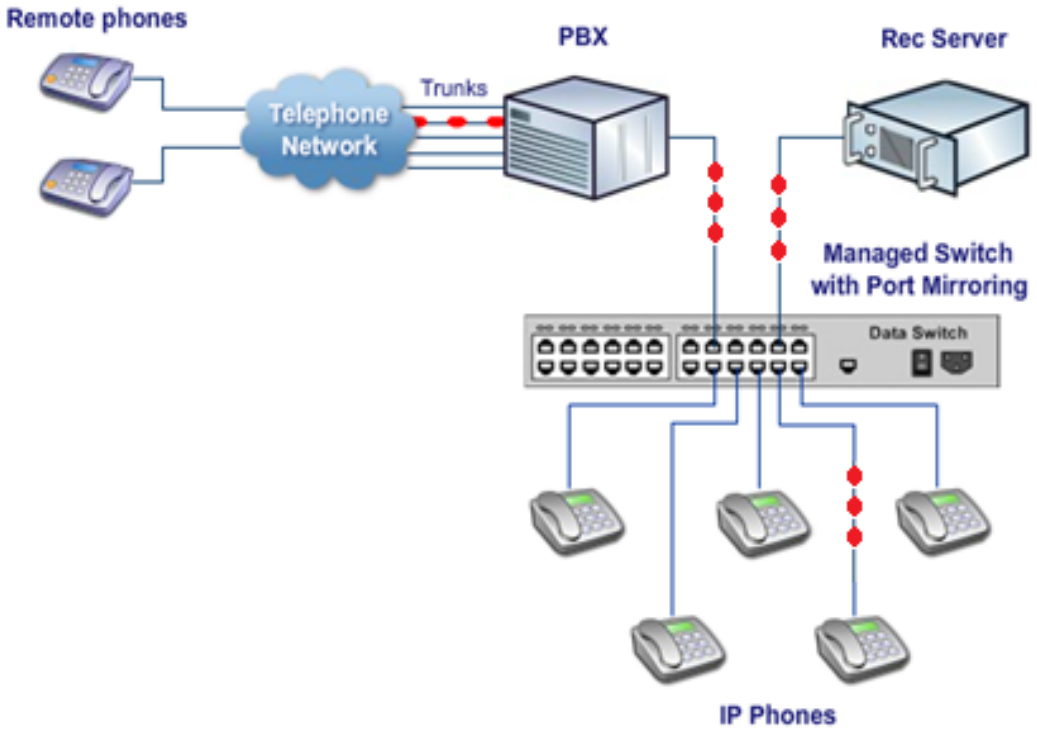
Computer D is a listener to the traffic. Computer D can be used for network logging or call recording if we have IP phones instead of computers A and B.

Conclusion: Port mirroring allows a computer to see the network traffic, which is normally hidden from it.

INTERACTION INSIGHT CORPORATION
GETTING YOU CLOSER TO YOUR CUSTOMERS

How the Port Mirroring function is used for VoIP call recording

The image below illustrates the usual configuration of network, which enables call recording.



In this example, an IP Phone makes a call to a remote phone outside of the local network (whether it is analog phone, cellular or another IP Phone).

Network traffic from IP Phone goes through network switch with port mirroring. The switch sends to the Recorder a copy of every network packet, sent or received by IP Phone.

By using intelligent packet capturing technology, the Recorder detects VoIP-related packets inside the network traffic, decodes them and saves audio on a disk.

Port Mirroring in different call scenarios

This overview contains some examples for "Port Mirroring" configuration on different types of VoIP network.

First of all it is necessary to decide which calls are required to be recorded.

There are three types of calls:

- **Outbound** (local phone makes a call to the external phone)
- **Inbound** (call is received from the external phone to the local phone)
- **Local** or **Internal** (call is established between two local phones)

If recording of local calls is not necessary (or there are no such calls), then a configuration of "Port Mirroring" is very simple.

You need to mirror the port, where the IP PBX is connected to (see Figure 1).

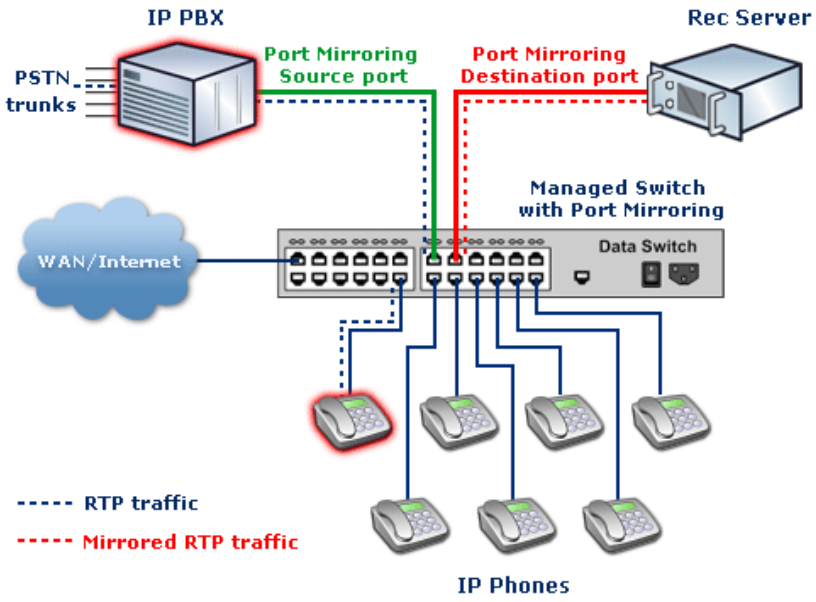


Figure 1. Recording of Inbound and Outbound calls only

On Figure 1 it is shown that RTP audio traffic is sent from IP Phone to IP PBX. This traffic is mirrored to the Recording server, where it is decoded.

This solution works for both inbound and outbound calls. But it may not work for local calls.

On most of IP PBX systems there is an optimization for network bandwidth usage: if the call is made between two local IP Phones, then RTP traffic is sent directly between phones without reaching the IP PBX (see Figure 2).

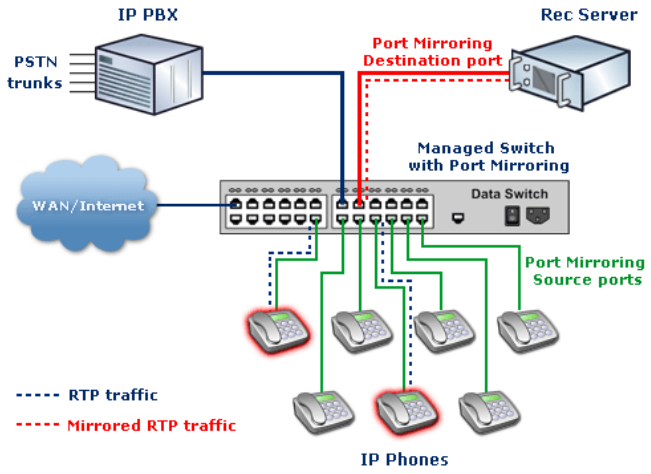


Figure 2. Recording of Inbound, Outbound and Local calls

In order to record Local calls as well as Inbound and Outbound it is necessary to mirror every port, where IP Phones are connected to.

Recording calls on the second switch

If IP Phones are connected through multiple switches, then additional effort is necessary to make call recording work. Configuration of "Port Mirroring" is easy if recording of local calls is not required. In this case "Port Mirroring" is required only on the main switch (see Figure 3).

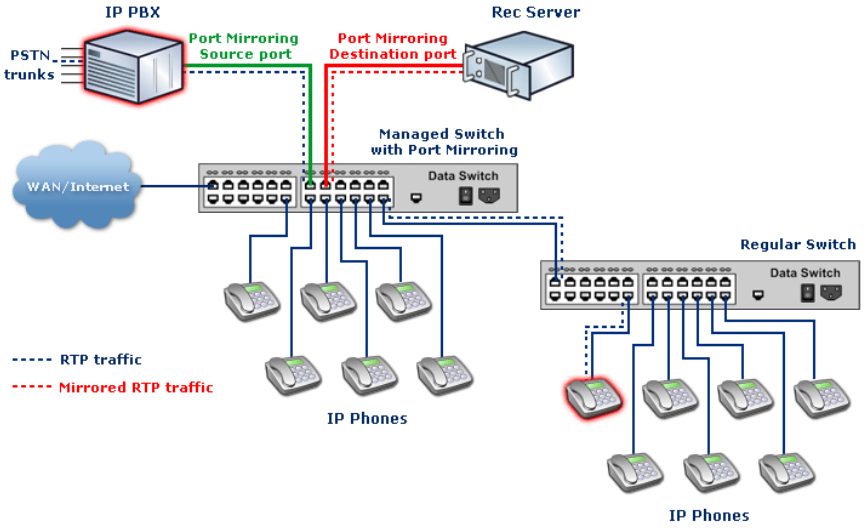


Figure 3. Recording of calls on the second switch

In the case that recording of local calls is required, then there are three solutions:

1. Install additional NIC into Recording server and connect multiple switches to it (see Figure 4)

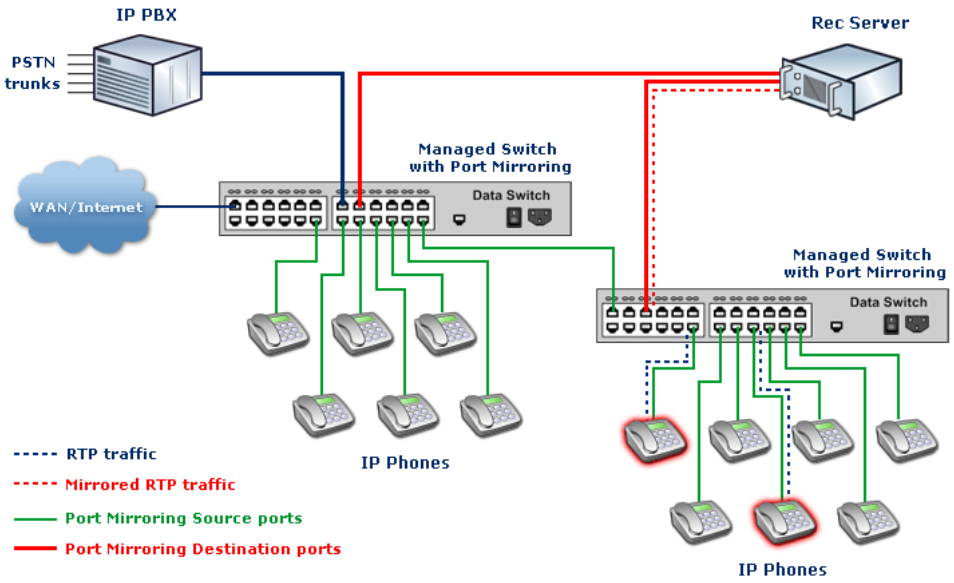


Figure 4. Recording server with two network adapters

2. Install a separate Recording server for the second switch (see Figure 5).

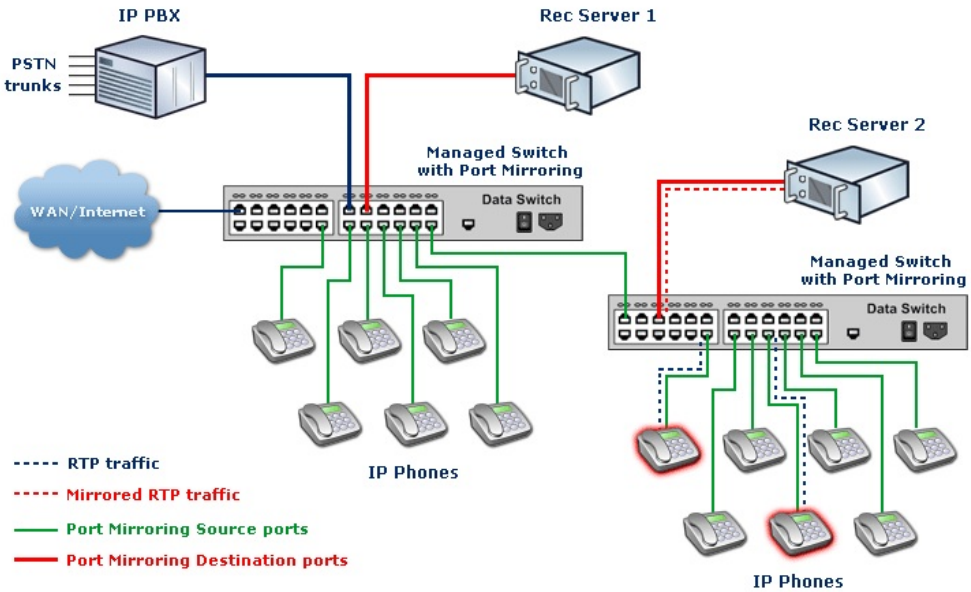


Figure 5. Two Recording servers

3. Use Remote SPAN (RSPAN) capability of Cisco Catalyst Switches (see Figure 6)

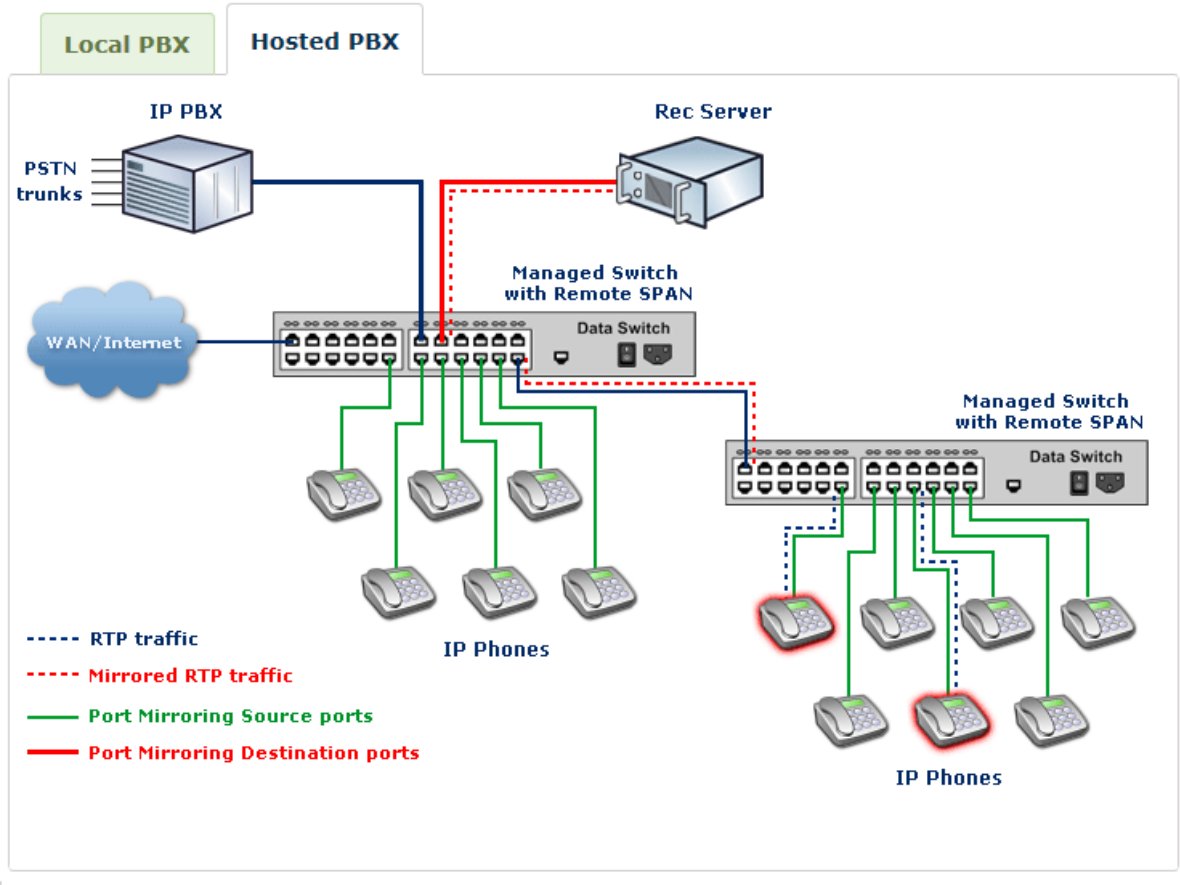


Figure 6. RSPAN configuration

RSPAN allows you to monitor source ports that are spread all over a switched network, not only locally on a switch with SPAN. This feature appears in CatOS 5.3 in the Catalyst 6500/6000 Series Switches and is added in the Catalyst 4500/4000 Series Switches in CatOS 6.3 and later.

The functionality works exactly as a regular SPAN session. The traffic that is monitored by SPAN is not directly copied to the destination port, but flooded into a special RSPAN VLAN. The destination port can then be located anywhere in this RSPAN VLAN. There can even be several destination ports.

More about RSPAN (link to Cisco web-site) >>

INTERACTION INSIGHT CORPORATION
GETTING YOU CLOSER TO YOUR CUSTOMERS

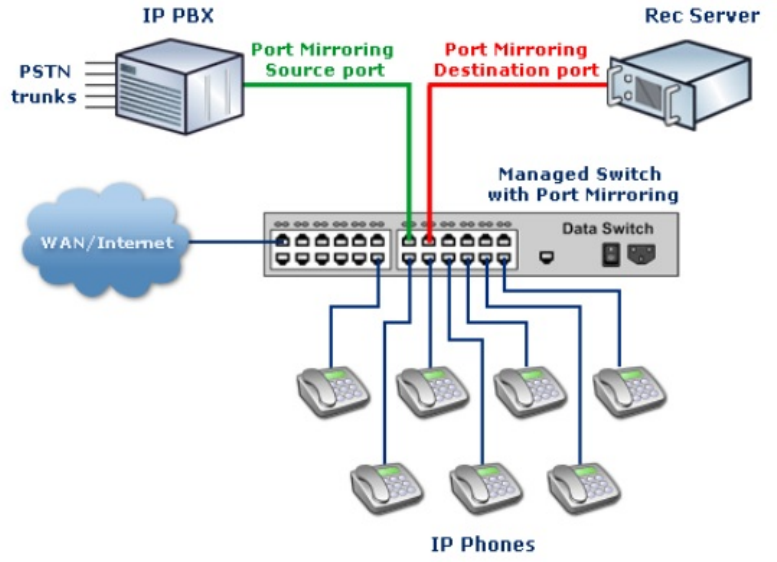
Port Mirroring Configuration Example - Cisco Catalyst 2960 Series Switches

This guide contains instructions for configuration of SPAN session (Port Mirroring) on **Cisco Catalyst 2960 Series Switches**.

Step 1. Connect all your devices like shown on following network diagram.

Local PBX Diagram

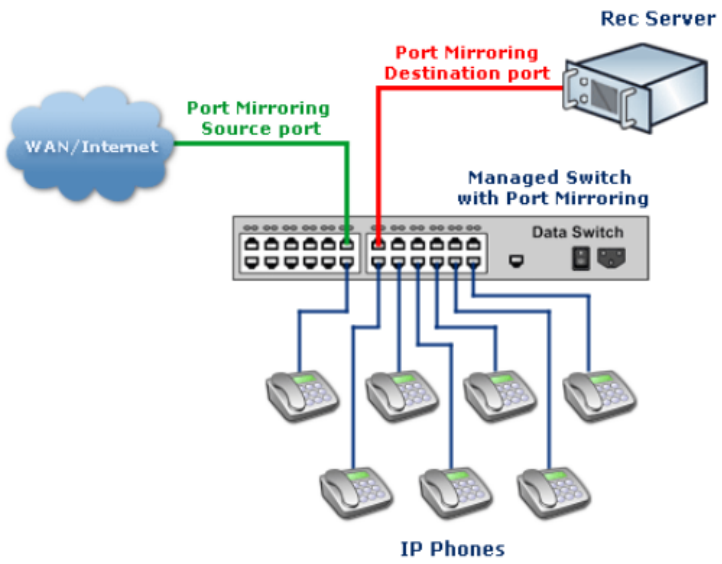
Local PBX | Hosted PBX



All IP Phones, for which a call recording is necessary, should be connected to Cisco Catalyst 2960 Series switch.

Hosted PBX Diagram

Local PBX | Hosted PBX



All IP Phones, for which a call recording is necessary, should be connected to Cisco Catalyst 2960 Series switch.

Step 2. Configure Port Mirroring function on the switch.

Let's assume the Rec Server is connected to **port 3**. On the network diagram it is shown in a red color (Analysis port).

And **port 5** is used for connecting to IP-PBX (if you have one) or uplink to WAN/Internet (if you do not have IP-PBX). On the network diagram it is shown in green color (Monitored port).

In this case you need to execute following command on the switch:

1. Enter configuration mode:

```
C2960# configure terminal
```

2. Create monitoring session and configure interface Fast Ethernet 0/5 as source port for that session:

```
C2960(config)# monitor session 1 source interface fastethernet 0/5
```

3. Configure interface Fast Ethernet 0/3 as destination port for session 1.

```
C2960(config)# monitor session 1 destination interface fastethernet 0/3
```

4. Check, if everything is configured correctly:

```
C2960# show monitor session 1

Session 1
---------
Source Ports:
 RX Only:       None
 TX Only:       None
 Both:          Fa0/5
Destination Ports: Fa0/3
```

Now a configuration is completed and you should be able to record calls.

Should you have any questions or issues, please, do not hesitate to contact our support team.

Caution! If you have inter-office calls (between local phones), then every phone's port should be set as a Source Port (Cisco Catalys 2960 switches supports monitoring of multiple ports).

You will need to execute command in point 2 (see above example) multiple times for every port:

```
C2960# configure terminal

C2960(config)# monitor session 1 source interface fastethernet 0/6
C2960(config)# monitor session 1 source interface fastethernet 0/7
C2960(config)# monitor session 1 source interface fastethernet 0/8
C2960(config)# monitor session 1 source interface fastethernet 0/9
C2960(config)# monitor session 1 source interface fastethernet 0/10
C2960(config)# monitor session 1 destination interface fastethernet 0/3
```

That assumes you have 5 IP Phones and they are connected to ports 6, 7, 8, 9 and 10 on the switch and Recorder server is connected to port 3.

More detailed information about configuration of SPAN can be found on the Cisco web-site:

Catalyst Switched Port Analyzer (SPAN) Configuration Example

INTERACTION INSIGHT CORPORATION
GETTING YOU CLOSER TO YOUR CUSTOMERS

Firewall Configuration Overview

Configuration of firewalls consist of two steps:

1. Opening ports, which are used for accessing the Recorder from other computers on the network
   (List of ports depends on recording solution and can be obtained from Project Manager)
2. Enable packets pass-through for port mirroring traffic

Enable packets pass-through for port mirroring traffic

The Recorder leverages port mirroring function on the switch. Some firewalls may block the network packets, which are mirrored to the Recorder server because they think that such traffic is malicious as it is not originally destined to that server (this is a traffic from IP Phone to IP PBX rather than to the Recorder server).

This may cause one of the following issues:

- One-way audio (when only one side of conversation is recorded)
- No audio is recorded at all (both sides of conversation are not recorded).

Windows Firewall (included into Windows XP, Vista, 7, 2003, 2008) doesn't have such problem. It passes through the mirrored network traffic to the Recorder server.

Other firewalls may block such traffic. Some of them have a configuration option, which allows to pass-through the traffic. Usually such option is identified as "Allow network bridged connections" or "Allow Internet sharing".

In worse case firewall doesn't have any option for passing through the network traffic and the only possible solution is to disable the firewall (or replace that firewall with another model). Usually, such firewalls are built-in to antivirus packages.