

UPnP

Document revision 2.3 (January 14, 2008, 11:56 GMT)

This document applies to V3.0

Table of Contents

[Table of Contents](#)

[Summary](#)

[Specifications](#)

[Description](#)

[Additional Documents](#)

[Enabling Universal Plug-n-Play](#)

[Property Description](#)

[Notes](#)

[Example](#)

[UPnP Interfaces](#)

[Property Description](#)

[Notes](#)

[Example](#)

General Information

Summary

The MikroTik RouterOS supports Universal Plug and Play architecture for transparent peer-to-peer network connectivity of personal computers and network-enabled intelligent devices or appliances. UPnP builds enables these devices to automatically connect with one another and work together to make networking possible for more people.

Specifications

Packages required: *system*

License required: *level1*

Home menu level: */ip upnp*

Standards and Technologies: [TCP/IP](#), [HTTP](#), [XML](#), [IGD](#)

Hardware usage: *Not significant*

Description

UPnP enables data communication between any two devices under the command of any control device on the network. Universal Plug and Play is completely independent of any particular physical medium. It supports networking with automatic discovery without any initial configuration, whereby a device can dynamically join a network. DHCP and DNS servers are optional and will be used if available on the network. UPnP implements simple yet powerful NAT traversal solution, that enables the client to get full two-way peer-to-peer network support from behind the NAT.

There are two interface types for UPnP: internal (the one local clients are connected to) and external (the

one the Internet is connected to). A router may only have one external interface with a 'public' IP address on it, and as many internal interfaces as needed, all with source-NATted 'internal' IP addresses.

The UPnP protocol is used for many modern applications, like most of DirectX games, as well as for various Windows Messenger features (remote assistance, application sharing, file transfer, voice, video) from behind a firewall.

Additional Documents

Enabling Universal Plug-n-Play

Home menu level: */ip upnp*

Property Description

allow-disable-external-interface (yes | no; default: **yes**) - whether or not should the users be allowed to disable router's external interface. This functionality (for users to be able to turn the router's external interface off without any authentication procedure) is required by the standard, but as it is sometimes not expected or unwanted in UPnP deployments which the standard was not designed for (it was designed mostly for home users to establish their own local networks), you can disable this behavior

enabled (yes | no; default: **no**) - whether UPnP feature is enabled

show-dummy-rule (yes | no; default: **yes**) - this is to enable a workaround for some broken implementations, which are handling the absence of UPnP rules incorrectly (for example, popping up error messages). This option will instruct the server to install a dummy (meaningless) UPnP rule that can be observed by the clients, which refuse to work correctly otherwise

Notes

CAUTION: if you do not disable the **allow-disable-external-interface**, any user from the local network will be able (without any authentication procedures) to disable the router's external interface.

Example

To enable UPnP feature:

```
[admin@MikroTik] ip upnp> set enable=yes
[admin@MikroTik] ip upnp> print
      enabled: yes
allow-disable-external-interface: yes
      show-dummy-rule: yes
[admin@MikroTik] ip upnp>
```

UPnP Interfaces

Home menu level: */ip upnp interfaces*

Property Description

interface (*name*) - interface name UPnP will be run on

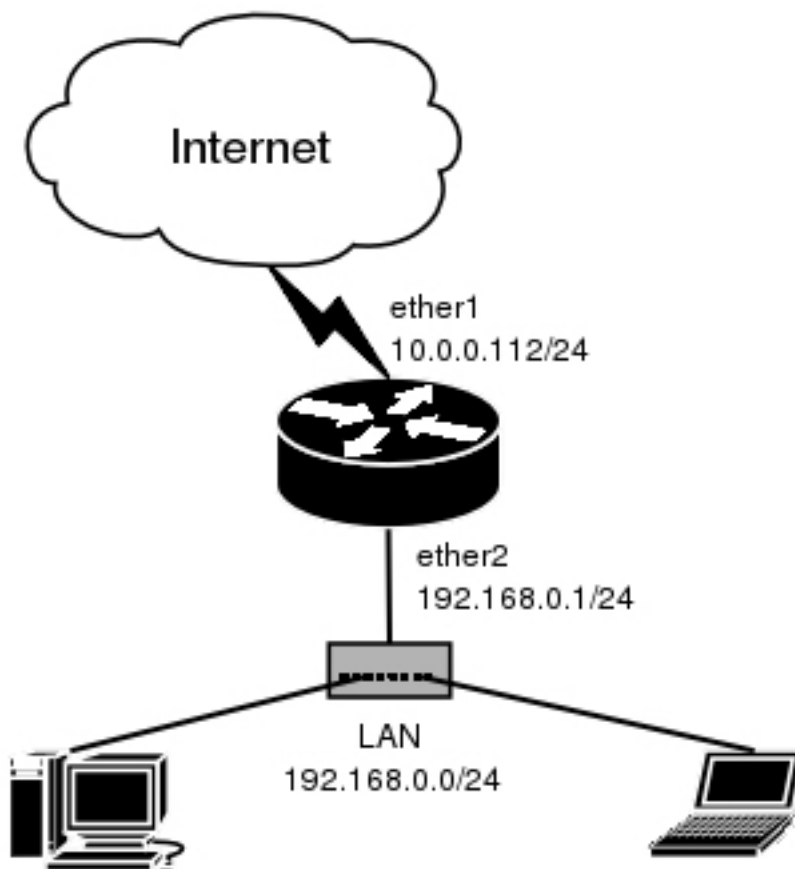
type (*external* | *internal*) - interface type, one of the:

- **external** - the interface a global IP address is assigned to
- **internal** - router's local interface the clients are connected to

Notes

It is highly recommended to upgrade DirectX runtime libraries to version [DirectX 9.0c](#) or higher and Windows Messenger to version [Windows Messenger 5.0](#) or higher in order to get UPnP to work properly.

Example



We have masquerading already enabled on our router:

```
[admin@MikroTik] ip upnp interfaces> /ip firewall src-nat print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=srcnat action=masquerade out-interface=ether1
[admin@MikroTik] ip upnp interfaces>
```

Now all we have to do is to add interfaces and enable UPnP:

```
[admin@MikroTik] ip upnp interfaces> add interface=ether1 type=external
[admin@MikroTik] ip upnp interfaces> add interface=ether2 type=internal
```

```
[admin@MikroTik] ip upnp interfaces> print
Flags: X - disabled
#  INTERFACE  TYPE
0 X ether1    external
1 X ether2    internal

[admin@MikroTik] ip upnp interfaces> enable 0,1
[admin@MikroTik] ip upnp interfaces> .. set enabled=yes
[admin@MikroTik] ip upnp interfaces>
```