

Regarding no ip forward-protocol udp



[gautamzone](#) 333 posts since

Jun 6, 2005

Dear All,

One of our client network has been audited and one of the audit measures suggested is to turn off unnecessary broadcasts caused due to the ip helper-address command on every L3 interface or SVI.

I am now planning to apply the following commands:

```
no ip forward-protocol udp tftp
```

```
no ip forward-protocol udp nameserver
```

```
no ip forward-protocol udp domain
```

```
no ip forward-protocol udp time
```

```
no ip forward-protocol udp netbios-ns
```

```
no ip forward-protocol udp netbios-dgm
```

However, my fear is that the IP address mentioned in the ip helper-address command is not only a DHCP server but also a DNS, WINS and NTP server.

So, will i be stopping communication by putting in the above commands.

Regarding no ip forward-protocol udp

Request for your clarification on this.



[Peter Paluch](#) 1,567 posts since

Jul 29, 2005 [Reply 1](#). **Re: Regarding no ip forward-protocol udp** Aug 19, 2009 6:11 AM

Hello Gautam,

Personally, I do not see a significant problem here. It is true that the IP Helper feature forwards several UDP broadcasts, including DNS, WINS, TFTP, and NTP. However, these services are nowadays used very rarely via broadcast. The DNS server is always obtained by static configuration or by DHCP. The same goes for the WINS server. The TFTP service is not usually used on workstations and the NTP is also not often used in broadcast mode. In other words, forwarding the broadcasts of these services is mostly useless and a sign of a bad implementation of that particular service.

Implementing these commands does not influence the operation of these services if they are accessed using unicasts instead of broadcasts. If your workstations are set up for a particular DNS, WINS and NTP server by its address then the services will continue working as usual. The IP Helper service is concerned exclusively with UDP broadcasts.

So I would say that you can apply the selected commands without greater risk. If a service fails to work properly after your changes, then I suggest changing the configuration of that service on the server and workstations.

Best regards,

Peter



[gautamzone](#) 333 posts since

Regarding no ip forward-protocol udp

Jun 6, 2005 [Reply 2. Re: Regarding no ip forward-protocol udp](#) Aug 19, 2009 8:28 AM

Thanks a lot Peter.

How about NETBIOS broadcast?

Can we disable that as well?

Thanks a lot again

Gautam



[Peter Paluch](#) 1,567 posts since

Jul 29, 2005 [Reply 3. Re: Regarding no ip forward-protocol udp](#) Aug 19, 2009 9:19 AM

Hello Gautam,

I believe you can disable the NetBIOS broadcast as well. Actually, the two NetBIOS services are the name service which is superseded by the WINS server that should be discovered by DHCP assignment, and the NetBIOS datagram service that is used for certain connectionless NetBIOS applications. None of these services needs to be forwarded beyond the local segment. Also note that if you are running the Active Directory domain, these services are largely obsolete. They were necessary in NT-style domains.

Try to see it from the other end: if we are talking about IP Helper and services to permit or deny, we are talking about services that use broadcasts for their normal work. Of all services that the IP Helper supports, only the DHCP **requires** forwarding the broadcasts to a central server if it is not on the same segment. All other services were originally designed to run per-segment and they did not assume that something ever forwarded the broadcasts to a central server. Therefore, turning off this broadcasting should not do any harm. Once again, the IP Helper absolutely does not influence any other traffic except the UDP broadcasts (and only selected services among those broadcasts).

Best regards,

Regarding no ip forward-protocol udp

Peter



[gautamzone](#) 333 posts since

Jun 6, 2005 [Reply 4. Re: Regarding no ip forward-protocol udp](#) Aug 22, 2009 12:38 PM

Thanks a lot Peter for the wonderful explanation.



[Peter Paluch](#) 1,567 posts since

Jul 29, 2005 [Reply 5. Re: Regarding no ip forward-protocol udp](#) Aug 22, 2009 1:00 PM

Gautam,

You are heartily welcome.

Best regards,

Peter