

RE: PortFast Question

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-09/0387.html>

LordInfidel_at_directionweb.com

Date: 09/27/04

To: 'Josh Sukol' <secnews@gmail.com>, security-basics@securityfocus.com
Date: Mon, 27 Sep 2004 10:16:00 -0400

If I had to guess..... the proprietary hardware box is having a hard time using auto-negotiation.

Here's what happens when you connect a device to a switch/hub, and both sides are set to auto-negotiate.

The connecting device will try to connect at it's maximum speed and duplex. If the other side(in this case the switch) can understand the connecting device and hence agree at the speed and duplex, the connection is made. If it can not understand the connecting device, it says Hey I can't understand that connection request, try another...

And they both go back and forth until a connection is made. Now there are times when a connection, "appears" to be made but you can not ping or it seems like the connection is really slow. That is because there are transmission errors due to the way each connection is expecting to receive the data.

Now with portfast, you are removing auto-negotiation from the switch and you are telling the switch port "Do not attempt to auto-negotiate, assume the port is 100/Full and bring the port up as such".

As far as protecting that port, you can lock that port down to the MAC address of the connecting device.

Typically, for any static network device that you are using, (servers, routers, firewalls, etc), the network adapter on the device should be manually set for speed/duplex. Never leave it set to auto.

-----Original Message-----

From: Josh Sukol [mailto:secnews@gmail.com]
Sent: Friday, September 24, 2004 10:05 AM
To: security-basics@securityfocus.com
Subject: PortFast Question

I am running a small network using four Cisco Catalyst 2950 switches. I am in the process of configuring a new software package that uses

SecurityFocus BASICS: RE: PortFast Question

some proprietary hardware that connects to the network via Ethernet. When plugged into the network the device would connect for a minute or two and then connectivity would drop (i.e. ping would fail, and the light on the switch would turn from green to amber) This pattern continued for as long as the device was plugged into the network. The cabling was checked and tested with other equipment and there were no other problems.

After trying several other things I eventually started changing the ethernet port settings on the switch itself and found that by enabling portfast the device functioned fine. I have found very little information about port fast security issues. I was able to find and did read up on PortFast BPDU guard and potential DoS using malformed packets. Are there any other security issues that effect me enabling Portfast on specific ports that connect back to a single device? Are there any other ways to solve this problem that might allow me to sidestep this potential security issues all together?

– Slightly Off Topic –

If anyone knows why this behavior occurs and why enabling portfast fixes the connectivity issue I would be very interested to a hear an explanation.

Thanks in advance for the wisdom!

Computer Forensics Training at the InfoSec Institute. All of our class sizes are guaranteed to be 12 students or less to facilitate one-on-one interaction with one of our expert instructors. Gain the in-demand skills of a certified computer examiner, learn to recover trace data left behind by fraud, theft, and cybercrime perpetrators. Discover the source of computer crime and abuse so that it never happens again.

http://www.infosecinstitute.com/courses/computer_forensics_training.html
