WAN Connectivity Troubleshooting

Company Logo Here

Introduction

Inter-office connectivity is provided by means of the Internet, which was designed to be a robust and self-healing network by providing multiple routes between locations. The flexibility by which a packet may take almost any route makes troubleshooting difficult, especially when a route is down and convergence is taking place.

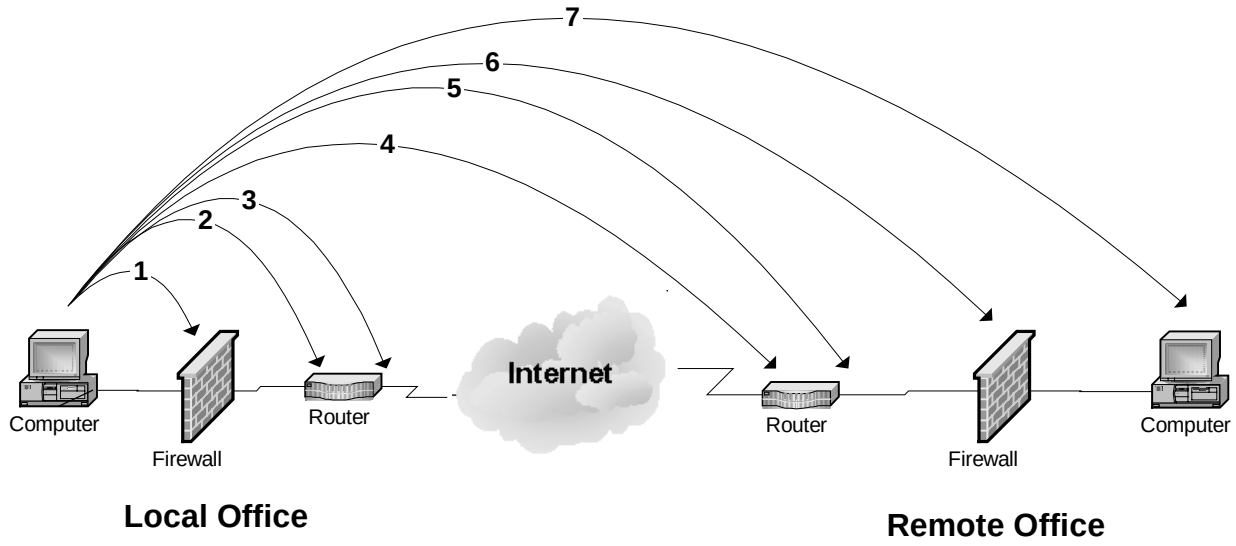
A fault may self-heal during a troubleshooting period depending on the extent of the routing problem. A simple route may self-heal in a matter of minutes thanks to the default 90-second routing update time of OSPF (a typical routing protocol). Where this has a knock-on effect onto multiple routers the time required obviously increases. As such you cannot assume that the result from a previous test has not changed during further troubleshooting.

All the following tests are non-destructive in nature and can be safely performed at any time by any member of staff from any machine. As there are no reboots involved there is no need to log device reboots.

It should also be noted that the offices are protected using firewalls, which prohibit ICMP (ping packets) to and from the Internet but do allow them between locations behind the firewalls.

The following are some brief tests that may be performed bearing the above in mind. The steps are numbered sequentially working away from the source and are not meant to indicate a more or less likely of point of failure.

Each step tests the connectivity at each point in the following diagram:



Step 1 – Testing of local firewall

This step tests that the firewall at the regional office is working correctly. Pinging the following local firewall should produce a response time <10ms.

Location	Firewall address
UK	1.1.1.253
**	2.2.2.253
**	3.3.3.253
**	4.4.4.253
**	5.5.5.253
**	6.6.6.253

Note that the above address is of the LAN side of the firewall so pings from inside the firewall should produce a reply. Pings from external sources (e.g. the local ISP should they attempt testing) will produce timeouts and is to be expected.

Result: *Failure to ping the local firewall should be followed by checking the physical connections to the firewall.*

Step 2 – Testing of local router (LAN)

This step tests that the router at the regional office is working correctly with respect to the LAN (Ethernet) connection.

It should be noted that the routers are outside of the firewalls and as such ping'ing from inside the firewalls will result in a timeout. Any pings from outside (e.g. the local ISP or another dialup service) should result in a reply.

As pings are blocked by the firewall so to perform basic testing of the router use the TELNET command followed by the router address shown below at the command prompt.

Location	CPE router address (LAN side)
UK	1.1.1.254
**	2.2.2.254
**	3.3.3.254
**	4.4.4.254
**	5.5.5.254
**	6.6.6.254

In most cases the local ISP manages the router and so although contact should be possible it will only be as far as the password login screen.

Note that under normal working conditions it should be possible to contact via telnet all the above routers from any office (this is tested in step 5).

Result: *If you are unable to telnet into the local router check the physical connections and also the LED's. In the case of the Cisco routers under normal conditions the LEDs should be as follows:*

Front/Top of router	
System PWR	On
System OK	On
WIC CD	On
WIC ACT	Flashing (rate depending on traffic)
LAN ACT	Flashing (rate depending on traffic)
LAN COL	Off (possibly some very low activity flashing)

Rear of router	
Flash PC card OK	On
10BaseT LNK	On
Serial CONN	On

For managed routers, beyond power resetting the router, troubleshooting should be escalated to the appropriate ISP.

Location	Local ISP	Contact Telephone number
UK	**	+** (0) **** **** ****
**	**	+** (0) **** **** ****
**	**	+** (0) **** **** ****
**	**	+** (0) **** **** ****
**	**	+** (0) **** **** ****
**	**	+** (0) **** **** ****

Step 3 – Testing of local router (WAN)

This step tests that the router at the regional office is working correctly with respect to the WAN (Serial) connection.

Exactly the same rules apply to this step as for step 2.

The address that telnet'ing to should be possible are as follows:

Location	CPE router address (WAN side)
UK	1.1.1.254
**	2.2.2.254
**	3.3.3.254
**	4.4.4.254
**	5.5.5.254
**	6.6.6.254

The same result as for step 2 should be expected and acted upon in the same manner.

Step 4 – Testing of remote router (WAN)

This step is the same as the test for step 3 but tests the connection to the router in the remote office that you are testing with respect to the remote WAN (Serial) connection.

Exactly the same rules apply to this step as for step 2.

For completeness the remote address that telnet'ing to should be possible are as follows:

Location	CPE router address (WAN side)
UK	1.1.1.254
**	2.2.2.254
**	3.3.3.254
**	4.4.4.254
**	5.5.5.254
**	6.6.6.254

The same result as for step 2 should be expected and acted on in the same manner.

Step 5 – Testing of remote router (LAN)

This step is the same as the test for step 32but tests the connection to the router in the remote office that you are testing with respect to the remote LAN (Ethernet) connection.

Exactly the same rules apply to this step as for step 2.

For completeness the remote address that telnet'ing to should be possible are as follows:

Location	CPE router address (WAN side)
UK	1.1.1.254
**	2.2.2.254
**	3.3.3.254
**	4.4.4.254
**	5.5.5.254
**	6.6.6.254

The same result as for step 2 should be expected and acted on in the same manner.

Step 6 – Testing of remote firewall

This step tests that the firewall at the remote regional office is working correctly. Pinging the following remote firewall should produce positive responses.

Using the "-t" switch on the PING command before the dotted address will perform the test until you hit CTRL+Break to allow for any normal timeouts due to excessive network utilisation on the Internet. Ideally response times in the region of 100ms are desired however more realistically they may be expected in the 150ms-250ms region.

Location	Firewall address
UK	1.1.1.253
**	2.2.2.253
**	3.3.3.253
**	4.4.4.253
**	5.5.5.253
**	6.6.6.253

Note that the above address is of the LAN side of the firewall so pings from inside the firewall should produce a reply. Pings from external sources (e.g. the local ISP) will produce timeouts and is to be expected.

Result: *Failure to ping the local firewall should be followed by checking the physical connections to the firewall.*

Step 7 – Testing of inter-office server connectivity

This test checks the availability of remote servers. The following devices should be available during all normal operations.

Location	Dotted notation	FQDN
UK	1.1.1.1	server01.domain.org
	1.1.1.2	server02.domain.org
**	2.2.2.1	server03.domain.org
	2.2.2.2	server04.domain.org
**	3.3.3.1	server05.domain.org
	3.3.3.2	server06.domain.org
**	4.4.4.1	server07.domain.org
	4.4.4.2	server08.domain.org
**	5.5.5.1	server09.domain.org
	5.5.5.2	server10.domain.org
**	6.6.6.1	server11.domain.org
	6.6.6.2	server12.domain.org

As for step 6 using the "-t" switch on the PING command before the dotted address will perform the test until you hit CTRL+Break to allow for any normal timeouts due to excessive network utilisation. Tests should be first performed using the dotted notation to discount DNS lookup issues.

Note that as the devices are inside the firewall pings to the above from external sources (e.g. the local ISP or another dialup account) will produce timeouts. This is to be expected.

Result: *If you can successfully ping using the dotted notation but fail with the FQDN obtain the DNS servers used by the local machine by typing "***`IPCONFIG /ALL`***" at the command line prompt and then attempt to ping those addresses.*