



# Monitor network ports

ONTAP 9

NetApp  
February 20, 2026

# Table of Contents

- Monitor network ports ..... 1
  - Monitor the health of ONTAP network ports ..... 1
  - Monitor the reachability of ONTAP network ports ..... 2
- Learn about port usage on the ONTAP network ..... 6
  - Inbound traffic ..... 6
  - Outbound traffic ..... 7
- Learn about ONTAP internal ports ..... 9

# Monitor network ports

## Monitor the health of ONTAP network ports

ONTAP management of network ports includes automatic health monitoring and a set of health monitors to help you identify network ports that might not be suitable for hosting LIFs.

### About this task

If a health monitor determines that a network port is unhealthy, it warns administrators through an EMS message or marks the port as degraded. ONTAP avoids hosting LIFs on degraded network ports if there are healthy alternative failover targets for that LIF. A port can become degraded because of a soft failure event, such as link flapping (links bouncing quickly between up and down) or network partitioning:

- Network ports in the cluster IPspace are marked as degraded when they experience link flapping or loss of layer 2 (L2) reachability to other network ports in the broadcast domain.
- Network ports in non-cluster IPspaces are marked as degraded when they experience link flapping.

You must be aware of the following behaviors of a degraded port:

- A degraded port cannot be included in a VLAN or an interface group.

If a member port of an interface group is marked as degraded, but the interface group is still marked as healthy, LIFs can be hosted on that interface group.

- LIFs are automatically migrated from degraded ports to healthy ports.
- During a failover event, a degraded port is not considered as the failover target. If no healthy ports are available, degraded ports host LIFs according to the normal failover policy.
- You cannot create, migrate, or revert a LIF to a degraded port.

You can modify the `ignore-health-status` setting of the network port to `true`. You can then host a LIF on the healthy ports.

### Steps

1. Log in to the advanced privilege mode:

```
set -privilege advanced
```

2. Check which health monitors are enabled for monitoring network port health:

```
network options port-health-monitor show
```

The health status of a port is determined by the value of health monitors.

The following health monitors are available and enabled by default in ONTAP:

- Link-flapping health monitor: Monitors link flapping

If a port has link flapping more than once in five minutes, this port is marked as degraded.

- L2 reachability health monitor: Monitors whether all ports configured in the same broadcast domain have L2 reachability to each other

This health monitor reports L2 reachability issues in all IPspaces; however, it marks only the ports in the cluster IPspace as degraded.

- CRC monitor: Monitors the CRC statistics on the ports

This health monitor does not mark a port as degraded but generates an EMS message when a very high CRC failure rate is observed.

Learn more about `network options port-health-monitor show` in the [ONTAP command reference](#).

3. Enable or disable any of the health monitors for an IPspace as desired by using the `network options port-health-monitor modify` command.

Learn more about `network options port-health-monitor modify` in the [ONTAP command reference](#).

4. View the detailed health of a port:

```
network port show -health
```

The command output displays the health status of the port, `ignore health status setting`, and list of reasons the port is marked as degraded.

A port health status can be `healthy` or `degraded`.

If the `ignore health status setting` is `true`, it indicates that the port health status has been modified from `degraded` to `healthy` by the administrator.

If the `ignore health status setting` is `false`, the port health status is determined automatically by the system.

Learn more about `network port show` in the [ONTAP command reference](#).

## Monitor the reachability of ONTAP network ports

Reachability monitoring is built into ONTAP 9.8 and later. Use this monitoring to identify when the physical network topology does not match the ONTAP configuration. In some cases, ONTAP can repair port reachability. In other cases, additional steps are required.

### About this task

Use these commands to verify, diagnose, and repair network misconfigurations that stem from the ONTAP configuration not matching either the physical cabling or the network switch configuration.

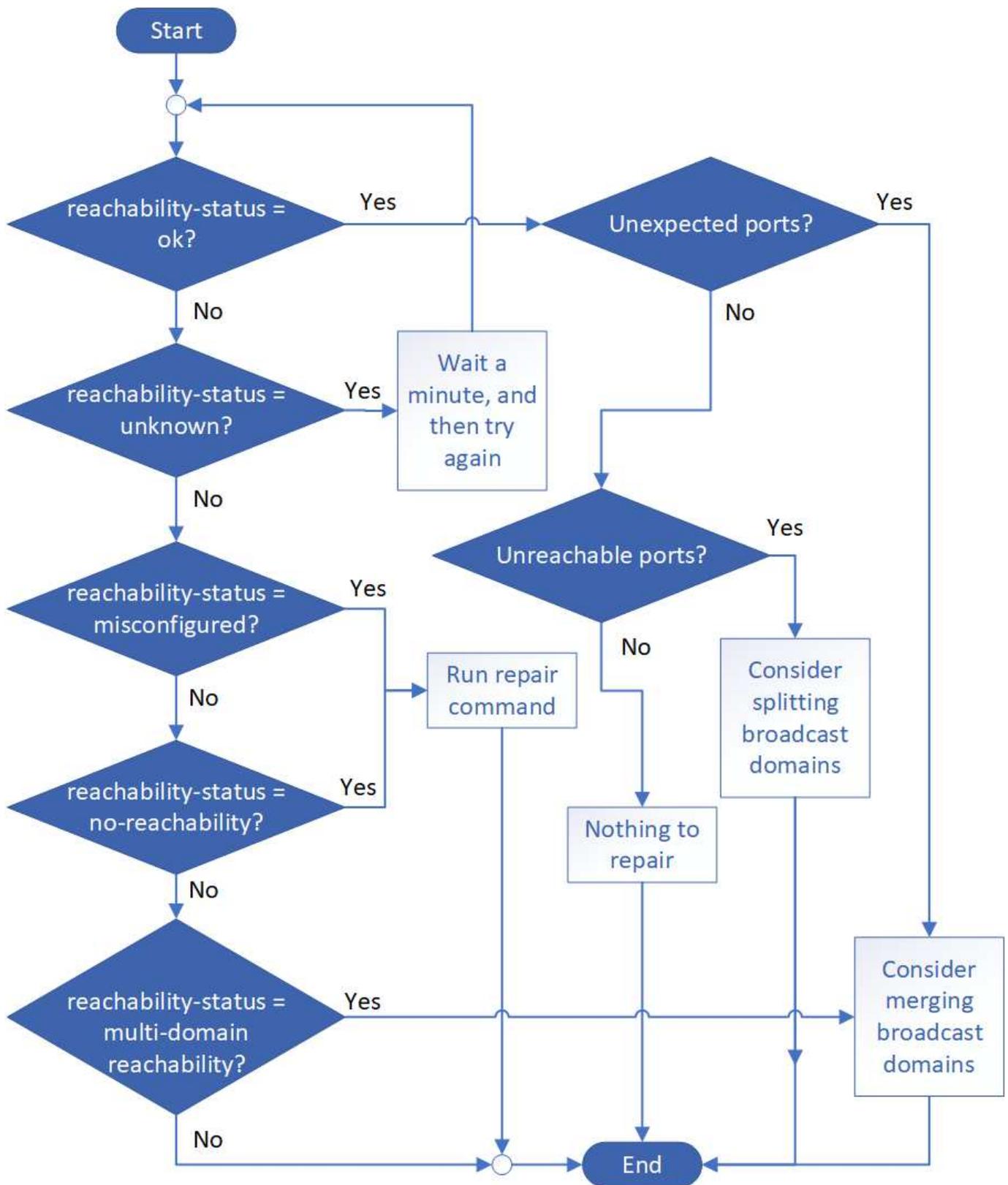
### Step

1. View port reachability:

```
network port reachability show
```

Learn more about `network port reachability show` in the [ONTAP command reference](#).

2. Use the following decision tree and table to determine the next step, if any.



Reachability-status	Description
---------------------	-------------

ok	<p>The port has layer 2 reachability to its assigned broadcast domain.</p> <p>If the reachability-status is "ok", but there are "unexpected ports", consider merging one or more broadcast domains. For more information, see the following <i>Unexpected ports</i> row.</p> <p>If the reachability-status is "ok", but there are "unreachable ports", consider splitting one or more broadcast domains. For more information, see the following <i>Unreachable ports</i> row.</p> <p>If the reachability-status is "ok", and there are no unexpected or unreachable ports, your configuration is correct.</p>
Unexpected ports	<p>The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain.</p> <p>Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains.</p> <p>For more information, see <a href="#">Merge broadcast domains</a>.</p>
Unreachable ports	<p>If a single broadcast domain has become partitioned into two different reachability sets, you can split a broadcast domain to synchronize the ONTAP configuration with the physical network topology.</p> <p>Typically, the list of unreachable ports defines the set of ports that should be split into another broadcast domain after you have verified that the physical and switch configuration is accurate.</p> <p>For more information, see <a href="#">Split broadcast domains</a>.</p>
misconfigured-reachability	<p>The port does not have layer 2 reachability to its assigned broadcast domain; however, the port does have layer 2 reachability to a different broadcast domain.</p> <p>You can repair the port reachability. When you run the following command, the system will assign the port to the broadcast domain to which it has reachability:</p> <pre>network port reachability repair -node -port</pre> <p>For more information, see <a href="#">Repair port reachability</a>.</p>
no-reachability	<p>The port does not have layer 2 reachability to any existing broadcast domain.</p> <p>You can repair the port reachability. When you run the following command, the system will assign the port to a new automatically created broadcast domain in the Default IPspace:</p> <pre>network port reachability repair -node -port</pre> <p>For more information, see <a href="#">Repair port reachability</a>.</p> <p>Learn more about <code>network port reachability repair</code> in the <a href="#">ONTAP command reference</a>.</p>

multi-domain-reachability	<p>The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain.</p> <p>Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains.</p> <p>For more information, see <a href="#">Merge broadcast domains</a> or <a href="#">Repair port reachability</a>.</p>
unknown	<p>If the reachability-status is "unknown", then wait a few minutes and try the command again.</p>

After you repair a port, you need to check for and resolve displaced LIFs and VLANs. If the port was part of an interface group, you also need to understand what happened to that interface group. For more information, see [Repair port reachability](#).

## Learn about port usage on the ONTAP network

Several well-known ports are reserved for ONTAP communications with specific services. Port conflicts occur if a port value in your storage network environment is the same as the value on an ONTAP port.

### Inbound traffic

Inbound traffic on your ONTAP storage uses the following protocols and ports:

Protocol	Port	Purpose
All ICMP	All	Pinging the instance
TCP	22	Secure shell access to the IP address of the cluster management LIF or a node management LIF
TCP	80	Web page access to the IP address of the cluster management LIF
TCP/UDP	111	RPCBIND, remote procedure call for NFS
UDP	123	NTP, network time protocol
TCP	135	MSRPC, Microsoft remote procedure call
TCP	139	NETBIOS-SSN, NetBIOS service session for CIFS
TCP/UDP	161-162	SNMP, simple network management protocol
TCP	443	Secure web page access to the IP address of the cluster management LIF
TCP	445	MS Active Domain Services, Microsoft SMB/CIFS over TCP with NetBIOS framing
TCP/UDP	635	NFS mount to interact with a remote file system as if it were local
TCP	749	Kerberos

UDP	953	Name daemon
TCP/UDP	2049	NFS server daemon
TCP	2050	NRV, NetApp remote volume protocol
TCP	3260	iSCSI access through the iSCSI data LIF
TCP/UDP	4045	NFS lock daemon
TCP/UDP	4046	Network status monitor for NFS
UDP	4049	NFS RPC Rquotad
UDP	4444	KRB524, Kerberos 524
UDP	5353	Multicast DNS
TCP	10000	Backup using Network Data Management Protocol (NDMP)
TCP	11104	Cluster peering, bi-directional management of intercluster communication sessions for SnapMirror
TCP	11105	Cluster peering, bi-directional SnapMirror data transfer using intercluster LIFs
SSL/TLS	30000	Accepts NDMP secure control connections between the DMA and NDMP server over secure sockets (SSL/TLS). Security scanners can report a vulnerability on port 30000.

## Outbound traffic

Outbound traffic on your ONTAP storage can be set up using basic or advanced rules depending on business needs.

### Basic outbound rules

All ports can be used for all outbound traffic over ICMP, TCP, and UDP protocols.

Protocol	Port	Purpose
All ICMP	All	All outbound traffic
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

### Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by ONTAP.

#### Active Directory

Protocol	Port	Source	Destination	Purpose
----------	------	--------	-------------	---------

TCP	88	Node management LIF, data LIF (NFS, CIFS, iSCSI)	Active Directory forest	Kerberos V authentication
UDP	137	Node management LIF, data LIF (NFS, CIFS)	Active Directory forest	NetBIOS name service
UDP	138	Node management LIF, data LIF (NFS, CIFS)	Active Directory forest	NetBIOS datagram service
TCP	139	Node management LIF, data LIF (NFS, CIFS)	Active Directory forest	NetBIOS service session
TCP	389	Node management LIF, data LIF (NFS, CIFS)	Active Directory forest	LDAP
UDP	389	Node management LIF, data LIF (NFS, CIFS)	Active Directory forest	LDAP
TCP	445	Node management LIF, data LIF (NFS, CIFS)	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
TCP	464	Node management LIF, data LIF (NFS, CIFS)	Active Directory forest	Change and set the Kerberos V password (SET_CHANGE)
UDP	464	Node management LIF, Data LIF (NFS, CIFS)	Active Directory forest	Kerberos key administration
TCP	749	Node management LIF, Data LIF (NFS, CIFS)	Active Directory forest	Change and set the Kerberos V password (RPCSEC_GSS)

#### AutoSupport

Protocol	Port	Source	Destination	Purpose
TCP	80	Node management LIF	support.netapp.com	AutoSupport (only if the transport protocol is changed from HTTPS to HTTP)

#### SNMP

Protocol	Port	Source	Destination	Purpose
TCP/UDP	162	Node management LIF	Monitor server	Monitoring by SNMP traps

#### SnapMirror

Protocol	Port	Source	Destination	Purpose
TCP	11104	Intercluster LIF	ONTAP intercluster LIFs	Management of intercluster communication sessions for SnapMirror

## Other services

Protocol	Port	Source	Destination	Purpose
TCP	25	Node management LIF	Mail server	SMTP alerts, can be used for AutoSupport
UDP	53	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
UDP	67	Node management LIF	DHCP	DHCP server
UDP	68	Node management LIF	DHCP	DHCP client for first-time setup
UDP	514	Node management LIF	Syslog server	Syslog forward messages
TCP	5010	Intercluster LIF	Backup endpoint or restore endpoint	Back up and restore operations for the Backup to S3 feature
TCP	18600 to 18699	Node management LIF	Destination servers	NDMP copy

## Learn about ONTAP internal ports

The following table lists the ports that ONTAP uses internally and their functions. ONTAP uses these ports for various functions, such as establishing intracluster LIF communication.

This list is not exhaustive and might vary in different environments.

Port/Protocol	Component/function
514	Syslog
900	NetApp Cluster RPC
902	NetApp Cluster RPC
904	NetApp Cluster RPC
905	NetApp Cluster RPC
910	NetApp Cluster RPC
911	NetApp Cluster RPC
913	NetApp Cluster RPC
914	NetApp Cluster RPC
915	NetApp Cluster RPC
918	NetApp Cluster RPC
920	NetApp Cluster RPC
921	NetApp Cluster RPC
924	NetApp Cluster RPC

925	NetApp Cluster RPC
927	NetApp Cluster RPC
928	NetApp Cluster RPC
929	NetApp Cluster RPC
930	Kernel services and management functions (KSMF)
931	NetApp Cluster RPC
932	NetApp Cluster RPC
933	NetApp Cluster RPC
934	NetApp Cluster RPC
935	NetApp Cluster RPC
936	NetApp Cluster RPC
937	NetApp Cluster RPC
939	NetApp Cluster RPC
940	NetApp Cluster RPC
951	NetApp Cluster RPC
954	NetApp Cluster RPC
955	NetApp Cluster RPC
956	NetApp Cluster RPC
958	NetApp Cluster RPC
961	NetApp Cluster RPC
963	NetApp Cluster RPC
964	NetApp Cluster RPC
966	NetApp Cluster RPC
967	NetApp Cluster RPC
975	Key Management Interoperability Protocol (KMIP)
982	NetApp Cluster RPC
983	NetApp Cluster RPC
5125	Alternate Control Port for disk
5133	Alternate Control Port for disk
5144	Alternate Control Port for disk
65502	Node scope SSH
65503	LIF Sharing
7700	Cluster Session Manager (CSM)
7810	NetApp Cluster RPC

7811	NetApp Cluster RPC
7812	NetApp Cluster RPC
7813	NetApp Cluster RPC
7814	NetApp Cluster RPC
7815	NetApp Cluster RPC
7816	NetApp Cluster RPC
7817	NetApp Cluster RPC
7818	NetApp Cluster RPC
7819	NetApp Cluster RPC
7820	NetApp Cluster RPC
7821	NetApp Cluster RPC
7822	NetApp Cluster RPC
7823	NetApp Cluster RPC
7824	NetApp Cluster RPC
7835-7839 and 7845-7849	TCP ports for intracluster communication
8023	Node Scope TELNET
8443	ONTAP S3 NAS port for Amazon FSx
8514	Node Scope RSH
9877	KMIP Client Port (Internal Local Host Only)
10006	TCP port for HA interconnect communication

## Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.