

Director Release Notes

Introduction

For further information about the Director Data Monitoring Switch and its software, visit www.netoptics.com, or contact Net Optics Technical Operations at (408) 737-7777 or ts-support@netoptics.com.

Director 2.2.0 Release Notes

This section contains release information about Director v2.2.0. The main purpose of this release is to provide support for SNMP, RADIUS, and TACACS+.

For detailed information about any of the new features, see the Director User Guide (Rev D) and CLI Command Reference (Rev A).

Release Contents

Image	dir_020200_070109 (~12.5M)
Documentation	Director Release Notes (this document) Director Quick Install guide Director User Guide Rev D Director CLI Command Reference Rev A

SNMP MIB

Director 2.2.0 provides the ability to manage Director using the SNMP protocol. The MIB includes the following tables:

- remoteSystemTable
- systemInfoTable
- sfUpgradeTable
- userTable
- portable
- portStatTable
- confParamTable
- v4ActiveFilterTable
- v4PendingFilterTable
- v6ActiveFilterTable
- v6PendingFilterTable
- filterAction

Features not available through the MIB at this time include filter utilization and Jumbo, CRC, and LFD modes.

SNMP Security

Director 2.2.0 support creation of SNMP security accounts. authProtocol is MD5 only, and privProtocol and user privilege levels are not supported. SNMP security is compatible with SNMPv1, SNMPv2, and SNMP3.

SNMP Traps

Director 2.2.0 generates traps to a single SNMP manager IP address for the following events:

- Cold and warm start
- Change of link state from up to down or down to up, all links (standalone units only; not available in multi-unit daisy-chained systems)
- Change of link state from up to down or down to up for the inter-unit daisy-chain links in multi-unit daisy-chained systems

The SNMP traps are compatible with SNMPv1 and SNMPv2.

RADIUS and TACACS+ Server Support

Director 2.2.0 supports user authentication and authorization through RADIUS and TACACS+ servers. Up to three of each server type can be specified, and server query sequence is configurable. Internal Director user accounts are always tried first, before going to any of the RADIUS and TACACS+ servers.

Additional Changes

Director 2.1.0 includes the following additional changes.

Item	ID	Feature or enhancement	Description
1	263	Added SSH and Web security key management	User can now generate a Web RSA key or SSH RSA key, import a Web RSA key and certificate, and export a Web Certificate Signing Request (CSR); the Web Identity Certificate is now unique for each Director unit.
2	132	Added Alias feature	User can now assign aliases for CLI commands and argument values.
3	169	Added user-defined filters (UDFs)	UDFs enable the user to specify a pattern of up to 16 contiguous bytes within the first 128 bytes of the packet as filter qualifier. A mask is supported to provide bitwise “don’t care” values. Limitations: <ul style="list-style-type: none"> • All UDFs in a system share the same offset and length • UDFs cannot be combined with any other filter parameters within a filter
4	313	Added a new SSH user account	Add a director SSH user account in addition to customer ; the default password for both accounts is netoptics .
5	285	Enhanced CLI confirmation prompts	CLI now accepts y , Y , n and N in addition to yes and no for confirmation prompts for the

			commands restart , logout , quit , and exit .
6	201	Speeded up gathering of port statistics for the Web Manager Statistics tab	Web Manager Statistics tab response time is now virtually instant.

Limitations

Director 2.2.0 has the following limitations:

1. No new functionality was added to the beta Web Manager (except that the gathering of port statistics was speeded up); it still does not include the functionality to configure and manage multi-unit systems, and the new features introduced in this release are available only through the CLI.
2. The maximum number of concurrent CLI sessions is now sixteen.

Known issues

Director 2.1.0 has the following issues:

1. Restrictions for user-defined filters:
 - udf_val and udf_mask must both be specified in the filter (udf_mask does not have a default value)
 - The length of the udf_val and udf_mask strings must be the same, and must be an integral number of bytes; for example, udf_val=ffe is illegal because it is 1.5 bytes
2. A software upgrade operation may take 10 minutes or longer depending on the network traffic condition.
3. In a multi-unit system, there is no global view for filter resource utilization. The command **filter list uid=<uid>** shows filter utilization in a particular unit. If the utilization is shown as greater than 100 percent, it means that the Director unit cannot support all specified filters. Filters are implemented in the available resources in priority order; if filter resources are exceeded, lowest priority filters become inactive. Therefore, be sure to keep the filter resource utilization on all units under 100 percent.
4. Browsers give security warnings when Web Manager is accessed. Here's why. To ensure security, Web Manager accepts only HTTPS connections, and not HTTP. Director has a self-signed security certificate. Your browser may give you a warning that the certificate is invalid or not trusted, or that a secure connection cannot be established. These warnings can safely be disregarded when connecting to an appliance such as Director. You should follow the warning's prompts to continue, or to create an exception for your Director's IP address.

Director 2.1.0 Release Notes

This section contains release information about Director v2.1.0. The main purpose of this release is to integrate Web Manager with the multi-unit system functionality.

Release Contents

Image	dir_020100_043009 (~12.5M)
--------------	----------------------------

Documentation	Director Release Notes (this document) Director Quick Install guide Director User Guide Rev C
----------------------	---

Web Manager Integration

Director 2.1.0 combines the Web Manager feature from release 1.1.0 with the release 2.0.0 code base. Note that 2.1.0 supports multi-unit system operation from the CLI, but Web Manager works only with a single stand-alone unit.

Additional Changes

Director 2.1.0 includes the following additional changes.

Item	Feature or enhancement	Description
1	Change remote mode while unit is cabled	It is no longer a requirement that a unit's daisy-chain (rear 10 Gigabit) ports be unconnected when the units remote mode is enabled or disabled with the remote set admin=<enable disable> command. It is also unnecessary to power cycle the unit after a mode change.
2	VLAN tags passed on 10 Gigabit ports	VLAN tags are no longer stripped from traffic on 10 Gigabit ports when using a valid VALN ID.
3	The range of valid VLAN IDs is now 2 to 4094	VLAN IDs 0, 1, and 4095 are not accepted because they are reserved according to IEEE 802.1Q (in addition, packets with VLAN IDs 0, 1, and 4095 have their VLAN tags stripped before being sent to monitor ports)
4	Web Manage access uses HTTPS	For system security, HTTP is not permitted for Web Manager access NOTE: Web Manager must now be invoked with https:// prefixing the IP address, for example, https://10.4.2.1

Limitations

Director 2.1.0 has the following limitations:

- Web Manager does not include the functionality to configure and manage multi-unit systems. It only handles single-unit stand-alone systems at this time.
- The maximum number of concurrent CLI sessions is seven.

Known issues

Director 2.1.0 has the following issues:

- Opening multiple CLI sessions impacts Web Manager performance.
- A software upgrade operation may take 10 minutes or longer depending on the network traffic condition.

9. In a multi-unit system, there is no global view for filter resource utilization. The command **filter list uid=<uid>** shows filter utilization in a particular unit. If the utilization is shown as greater than 100 percent, it means that the Director unit cannot support all specified filters. Filters are implemented in the available resources in priority order; if filter resources are exceeded, lowest priority filters become inactive. Therefore, be sure to keep the filter resource utilization on all units under 100 percent.
10. Browsers give security warnings when Web Manager is accessed. Here's why. To ensure security, Web Manager accepts only HTTPS connections, and not HTTP. Director has a self-signed security certificate. Your browser may give you a warning that the certificate is invalid or not trusted, or that a secure connection cannot be established. These warnings can safely be disregarded when connecting to an appliance such as Director. You should follow the warning's prompts to continue, or to create an exception for your Director's IP address.

Director 2.0.0 Release Notes

This section contains release information about Director v2.0.0. The main purpose of this release is to support operation of multi-unit systems in a daisy-chain topology.

Release Contents

Image	dir_020000_033109
Documentation	Director Release Notes (this document) Director Multi-Unit Systems Quick Start card Director User Guide Rev B

Multi-unit (Daisy-chained) System Operation

Director 2.0.0 provides the capability to connect up to 10 Director units in a daisy-chain that operates as a single logical system. To support this function the following changes are made to the CLI.

item	Feature or enhancement	Description
1	Added new CLI command: remote set admin=<enable disable> master=<enable disable>	The admin parameter enables a Director unit for multi-unit operation. The master parameter assigns a particular Director unit as the <i>master</i> for the multi-unit system. The rest of the units are <i>slave</i> or <i>remote</i> units. The master must be the first unit on the daisy-chain.
2	Added new CLI command: remote group topology= <n1,n2,...>	This parameter defines the daisy-chain topology for the number of units in the multi-unit system. Example: remote group topology=1,2 for a two-unit system.
3	Added new CLI command: remote commit	This command saves the specified remote configuration (topology) in an internal database and transmits it to all of the units in the system.
4	Added new CLI command: remote show	This command displays the remote configuration and status, including the status of each unit in the system.

5	Added new CLI parameter: module show uid=<uid>	This command displays the hardware status of the specified unit in a multi-unit system.
6	Added new CLI parameter: port show uid=<uid>	This command displays the port status of the specified unit in a multi-unit system.
7	Added new CLI parameter: port set uid=<uid>	This command configures the port settings of the specified unit in a multi-unit system.
8	Added new CLI parameter: stats show uid=<uid>	This command displays the port statistics of the specified unit in a multi-unit system.
9	Added new CLI parameter: stats clear uid=<uid>	This command clears the port statistics of the specified unit in a multi-unit system.
10	Extended address nomenclature to support multi-unit systems.	To create filters that involve remote units in a multi-unit system, prefix the port number with the UID. For example, u2.n1.1 is the first network port on the second unit in the daisy-chain. Ports in the master unit can be prefixed with "u1." or the prefix may be omitted.

Limitations

Director 2.0.0 has the following limitations:

1. When configuring a multi-unit system, please follow the instructions in the User Guide. It is important that units must not have their daisy-chain ports connected (cabled to another unit) when **remote=<enable|disable>** mode changes are made.
2. The maximum amount of network and monitor traffic that can be carried between units in a multi-unit system is 9 Gigabits per second. Packets are dropped when traffic exceeds this amount. The reason why this bandwidth is not 10 Gigabits is that one Gigabit is needed for the overhead of inter-unit communications.

Known issues

Director 2.0.0 has the following issues:

1. Dynamic **remote=<enable|disable>** mode changes made when cables are connected between units may cause a faulty internal state. If this happens, cycle power on all of the units in the system to recover.
2. VLAN tags are stripped from traffic on 10 Gigabit ports.
3. There is no global view for filter resource utilization in a multi-unit system. The **command filter list uid=<uid>** shows filter utilization in a particular unit. If the utilization is shown as greater than 100 percent, it means that the Director unit cannot support all specified filters. Filters are implemented in the available resources in priority order; if filter resources are exceeded, lowest priority filters become inactive. Therefore, be sure to keep the filter resource utilization on all units under 100 percent.
4. A problem was seen once in testing where an unstable Link Fault Detect (LFD) on a Copper In-Line DNM may have interfered with management traffic between units in a multi-unit system. This problem is under investigation. Work-around: If a multi-unit system is having problems, try turning off LFD and seeing if it fixes it.

Director 1.1.0 Release Notes

This section contains release information about Director 1.1.0. The main purpose of this release is to provide a Beta version of Web Manager, Director's Web-browser based management software.

Release Contents

Image	dir_010100_033109
Documentation	Director Release Notes (this document) Director User Guide, System Manager Beta

Web Manager

Director 1.1.0 provides a Beta version of Web Manager, Director's Web-browser based management software. To access Web Manager, type the IP address of the Director unit into your browser's address bar.

CRC Forwarding

Director 1.1.0 provides the capability to enable passing packets that have CRC errors to the redirect ports. This feature is off by default. To enable CRC Forwarding, use the following CLI command: **system set crc=< on | off >**. This setting is global for all of the units in a multi-unit system.

Known issues

Director 1.1.0 has the following issues:

1. When upgrading Director software over the Internet using either the CLI or Web Manager, the upgrade command may time out if the Internet is congested.

Work-arounds:

- a. Start the upgrade process in the morning or at night when the Internet is likely to be less busy.
 - b. Setup an ftp server on a local intranet. Put the new image on the ftp server and then upgrade from that server rather than over the Internet. (This is the most reliable solution.)
 - c. When an upgrade timeout happens, ignore the error and wait for 15 minutes; then restart the system using the system restart command in the CLI.
2. The Beta version of Web Manager has no error messages.