New and Changed Information

See the Workflow document to refer the other guides of NCS 1002.

This table summarizes new and changed information for configuration guide for Release 6.3.2, and lists where the features are documented.

Table 1: New and Changed Features - R6.3.2

Feature	Description	Where Documented
GMPLS UNI Flexible Grid	The user can create a GMPLS optical channel trail (OCH Trail) in a network where the NCS 1002 node is connected to a NCS 2000 series node. GMPLS UNI flexible grid is supported from R6.3.2 that supports 250G channels and 6.25 GHz channel spacing.	Configuring GMPLS UNI
IPv6 ACL	NCS 1002 supports the following IP Acces List (ACL): • Ingress ACL for both IPv4 and IPv6. • Egress ACL: Self-Originated Packet is not supported by ACL, as this is already controlled by user. Only forwarded packets or traffic is classified under ACL. This rule is applicable for both IPv4 and IPv6 ACL.	Configure IP Accesss List
MACsec SNMP	The following MIB is supported in NCS 1002. IEEE8021-SECY-MIB (only SNMP read-only operations are supported for this MIB).	Configuring SNMP

Feature	Description	Where Documented
MACsec Threshold Crossing Alerts	The user can configure MACsec Threshold Crossing Alerts (TCA) at mac-sec ether, secy-if (interface), secy-tx,and secy-tx. There is no default threshold, minimum, or maximum threshold to configure MACsec TCA. The user must enable MACsec controllers to view MACsec performance. To configure MACsec threshold crossing alerts and the performance monitoring parameters, see the Configuring MACsec Encryption chapter in the Configuration Guide for Cisco NCS 1002.	Configuring MACsec Threshold Crossing Alerts
MACsec MKA Using EAP-TLS Authentication	Using IEEE 802.1X port-based authentication with Extensible Authentication Protocol (EAP-TLS), MACsec MKA can be configured between two NCS 1002 device ports. EAP-TLS allows mutual authentication and obtains MSK (master session key or primary session key). Both Connectivity Association Key Name (CKN) and connectivity association key (CAK) are derived from MSK for MKA operations. The device certificates are carried for authentication to the external AAA server using EAP-TLS.	MACsec MKA Using EAP-TLS Authentication
Mixed Mode Configuration	The first three client ports of a slice can be configured at 100G bitrate and the last two client ports can be configured at 10G bitrate per lane. This feature is called mixed mode configuration.	Configuring Slices

Feature	Description	Where Documented
PRBS	Pseudo Random Binary Sequence (PRBS) feature allows the user to perform data integrity checks between the trunk links of NCS 1002 without enabling the client traffic. PRBS generator generates a bit pattern on the device and sends it to the peer device, where PRBS analyzer detects if the transmitted bit pattern is preserved. The user can configure the trunk port in one of the following modes for PRBS. • Source Mode • Sink Mode • Source-Sink Mode	Pseudo Random Binary Sequence