This page was created to document important default configuration differences for IPv4 features and protocols between the Cisco NX-OS (Nexus 7000) and Cisco IOS Software (Catalyst 6500). The objective of this document is to point out key differences to insure success when installing a Nexus 7000 for the first time. Some of the default differences are based on architectural differences, whereas others are based on default configuration differences for features enabled by default and for features that are manually configured that are not enabled by default.

Additional Resources:

- The IOS/NX-OS Migration tool on cisco.com can be used to assist when converting a Cisco IOS Software configuration to a Cisco NX-OS Software configuration.
- Minimum Recommended Cisco NX-OS Releases for Cisco Nexus 7000 switches on cisco.com

Contents

- 1 Initial System Setup (First Time Boot-up)
- 2 Virtual Routing and Forwarding (VRF) Instances
- 3 Interface Parameters
- 4 Layer-2 Switching Features and Protocols
- 5 Layer 3 Features and Protocols
- 6 Layer-3 Unicast Routing Features and Protocols
- 7 Multicast Features and Protocols
- 8 MPLS Features and Protocols
- 9 Security Features and Protocols
- 10 Quality of Service Features
- 11 Network Management Features and Protocols

Initial System Setup (First Time Boot-up)

This section outlines the defaults that are applied to the configuration the first time the system boots up if the user chooses not to run the setup utility. Different features and parameters can be configured during the initial system startup if the user chooses to run the setup utility.

Device Access (Security)	Cisco NX-OS	Cisco IOS	Notes
Secure Password Standard	Yes	No	The Secure Password Standard forces the user to select a secure combination of characters (lower and upper case) and numbers.
Terminal (SSH/TELNET)	SSHv2	TELNET	Cisco NX-OS Software defaults to SSHv2 with a 1024 bit RSA key. The SSH key can be modified to a DSA/RSA key up to 2048 bits to increase security.
Local Authentication	**admin** user	Requires Additional	Cisco NX-OS Software prompts for an **admin** user password when the system is powered on for the first time,

		Configuration	whereas Cisco IOS Software uses a VTY and Console password with an Enable Secret to secure access (All passwords in Cisco IOS Software have to be configured).
CoPP Policy	Enabled	No	Cisco NX-OS Software defaults to the **strict** CoPP policy, which is the most restrictive policy to protect the control plane (CPU). The **strict** CoPP policy is recommended for most environments. Cisco IOS Software requires the administrator to create a CoPP policy and apply it to the control-plane.
Interface Configuration	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Port Type	Layer-3	Layer-3	Later versions of Cisco IOS Software define the port type as Layer-3, whereas earlier versions define the port type as Layer-2 by default.
Port State	Shutdown	Shutdown	Later versions of Cisco IOS Software shutdown all of the ports, whereas earlier versions enabled them by default.
Console / VTY Parameters	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Console Timeout	30 (minutes)	10 (minutes)	Later versions of the Cisco NX-OS Software have a 30 minute timeout enabled by default. The Cisco NX-OS console timeout value can be modified with the Console **exec-timeout** CLI command.
VTY Timeout (SSH/TELNET)	30 (minutes)	10 (minutes)	Later versions of the Cisco NX-OS Software have a 30 minute timeout enabled by default. The Cisco NX-OS VTY timeout value can be modified with the VTY **exec-timeout** CLI command.
VTY Session Limit	32	10	Later versions of Cisco IOS Software configure 10 VTY's by default, whereas earlier versions configure up to 16.

Additional Notes:

- The Cisco NX-OS Software setup utility can be executed anytime using the **setup** command in EXEC user mode.
- The port type is dependent on the module type. In Cisco NX-OS Software, the M1 series modules default to a layer-3 port type configuration and the F1 series modules default to a layer-2 port type configuration (F1 series modules only support layer-2 port types).
- The Cisco NX-OS Software default port state can be modified after the system is initially configured with the global **system default switchport** command.
- Early versions of Cisco NX-OS Software did not display the VTY interface in the running or startup configuration unless the default values were modified. Later versions display **line vty** in both the running and startup configurations.

Virtual Routing and Forwarding (VRF) Instances

This section outlines the default VRF instance configuration. The NX-OS has two VRF instances that are configured by default when the system is powered on for the first time. Additional VRF instances can be configured as required.

VRF Instance Name	Cisco NX-OS	Cisco IOS	Notes
Default (Global)	All I/O Ports	All I/O Ports	The **default** VRF instance in Cisco NX-OS Software is equivalent to the global VRF instance in Cisco IOS Software.
Management	Supervisor **mgmt0** port	N/A	Cisco NX-OS Software assigns the **mgmt0** port(s) on the Supervisor(s) to the **management** VRF instance (This cannot be modified).
Configuration	**Cisco NX-OS**	**Cisco IOS**	**Notes**
CLI Placement	Under VRF hierachy	Ussually uses **vrf** option	The CIsco NX-OS uses a more centric model when configuring protocols and features associated with VRF instances. For instance, protocols and features such as PIM and IP static routes are configured under the VRF context. Cisco IOS typically uses the **vrf** option to differentiate bewteen non-default VRF instances.

Additional Notes:

- Cisco NX-OS Software uses the **vrf member <vrf name>** interface command to associate an interface with a VRF instance, whereas Cisco IOS uses **vrf forwarding <vrf name>** interface command.
- In Cisco NX-OS Software, VRF instances are associated to routing protocols under the routing protocol with the **vrf** command. This is similar for some protocols in the Cisco IOS Software (i.e. BGP, EIGRP) that use address families under the routing protocol configuration.

Interface Parameters

This section outlines default configuration differences related to interface types and configuration parameters.

Interfaces	Cisco NX-OS	Cisco IOS	Notes
Link Debounce (Timer)	100 (ms)	3100 (ms)	The Link Debounce feature is disbled by default in both Cisco NX-OS and IOS Software. However, when enabled, the default timers are different. Cisco NX-OS Software allows the user to specify a non-default timer using the **time** option.
L2 Interfaces	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Switchport Mode	Access	Dynamic Desirable	Cisco IOS Software doesn't default to switchport access mode.
Switchhport Trunk Encapsulation	802.1q	Negotiate	The Cisco NX-OS Software only supports 802.1q Trunks - It cannot negotiate between ISL and 802.1q.
L3 Interfaces (IP)	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Proxy-ARP	Disabled	Enabled	Cisco NX-OS Software can enable Proxy-ARP per interface using the **ip proxy-arp** interface command.
Unreachables (ICMP)	Disabled	Enabled	

			Cisco NX-OS Software disables ICMP unreachable messages by default (Port ICMP unreachable messages are enabled by default), whereas the Cisco IOS Software enables all types of ICMP unreachable messages by default. IP unreachable messages can be enabled per interface in the Cisco NX-OS using the **ip unreachables** interface command.
VRF Instance	**default** Instance	Global Instance	The Cisco NX-OS Software puts all Layer-3 I/O interfaces into the **default** VRF instance.
Loopback Interfaces	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Interface Range	0-1023	0-2147483647	These values do not indicate the total number of loopback interfaces that can be configured. Check the latest documentation to determine how many loopback intefaces are supported per chassis.
Port-Channel Interfaces	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Interface Range	1-4096	1-256	These values do not indicate the total number of port-channel interfaces that can be configured. Check the latest documentation to determine how many port-channel interfaces are supported per chassis.
Interface State	Operational	Admin. Down	This is the default interface state after the port-channel interface is initially created.
LaCP Graceful-Convergence	Enabled	N/A	Applied per port-channel interface. This can be disabled in Cisco NX-OS Software using the **no lacp graceful-convergence** interface command (only recommended to disable this with non NX-OS LaCP neighbors).
LaCP Max-Bundle	16	8	-
LaCP Suspend-Individual	Enabled/Disabled	N/A	Applied per port-channel interface. This can be disabled in Cisco NX-OS Software using the **no lacp suspend-individual** interface command.The feature is enabled by default on the Nexus 7000 platform. Other Nexus Platforms (such as the 5000 series) have it disabled by default. This feature violates the LACP RFC. Disabling the feature is necessary for PXE boot scenarios where the booting software does not support LACP.
Tunnels Interfaces (GRE)	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Bandwidth	9 Kbps	100 kbps	The Cisco NX-OS Software tunnel interface bandwidth can be modified with the **bandwidth <#>** interface command.
Interface Range	0-4095	0-2147483647	These values do not indicate the total number of tunnel interfaces that can be configured. Check the latest documentation to determine how many tunnel interfaces are supported per

			chassis.
Interface State	Admin Down	Operational	This is the default interface state after the tunnel interface is initially created.
PMTU Discovery (Min MTU)	64 Bytes	92 Bytes	The Cisco NX-OS software Minimum MTU can be modified with the **tunnel path-mtu-discovery min-mtu** interface command
Time-To-Live (TTL)	Disabled	255	The Cisco NX-OS Software tunnel TTL value can be modified with the **tunnel ttl** interface command

Additional Notes:

- Tunnel interfaces are disabled by default in Cisco NX-OS Software. IP tunnel interfaces can be enabled with the **feature tunnel** command.
- Switch Virtual Interfaces (SVIs) are disabled by default in Cisco NX-OS Software and cannot be configured until the **feature interface-vlan** command is configured.

Layer-2 Switching Features and Protocols

This section outlines some key differences related to layer-2 switching features and protocols, such as VLANs, VTP, STP, etc...

VLAN Support/Ranges	**Cisco NX-OS**	**Cisco IOS**	**Notes**
VLAN Range	1-4094	1-4094	Cisco NX-OS Software supports 4094 VLANs per Virtual Device Context (VDC).
Extended VLANs	1006-4094	1006-4094	Cisco NX-OS Software does not require a CLI command to enable Extended VLANs.
Reserved for Internal Use	3968-4047,4094	1002-1118	As of Cisco NX-OS 5.2(1) the reserved internal VLAN range was expanded to use 128 VLANs (3968-4094) - In Cisco NX-OS 5.2(1), the global **system vlan <#> reserve** command can be configured to reserve a different range of VLANs.
MAC Table Aging Timer	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Default Aging Timer	1800 (seconds)	300 (seconds)	The MAC address table aging-timer can be modified in Cisco NX-OS Software with the global **mac address-table aging-time <0, 120-918000>** command. A value of **0** disables the aging timer.
STP Protocol Default	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Default STP	Rapid-PVST+	PVST	The STP protocols are backwards compatible, but it is recommended to configure all switches in an L2 domain to use the same STP.
VTP Default	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Mode	Disabled	Transparent	

			Cisco NX-OS Software drops all VTP packets by default (VTP can be configured for client, server or transparent mode).

Additional Notes:

- Extended VLANs cannot be shutdown or suspended in Cisco NX-OS or Cisco IOS Software.
- The Cisco NX-OS Software **show vlan internal usage** command lists all of the reserved VLANs.
- Later versions of Cisco IOS Software enable Extended VLANs by default with the global **spanning-tree extend system-id** command.
- The MAC table aging timer should be longer than the layer-3 ARP cache timer, so ARP updates refresh the MAC table entries.
- VTP is disabled by default in the Cisco NX-OS Software. VTP can be enabled with the global **feature vtp** command.

Layer 3 Features and Protocols

The following table outlines the default differences for layer-3 protocols other than Routing Protocols such as ARP, DHCP, etc...

ARP	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Default (Global)	1500 (seconds)	14400 (seconds)	In Cisco NX-OS Software, the ARP timeout can be modifed with the global **ip arp timeout <60 - 28800>** command.
DHCP Relay	**Cisco NX-OS**	**Cisco IOS**	**Notes**
DHCP Relay	Disabled	Enabled	Cisco NX-OS requires the **feature dhcp** and the **ip dhcp relay** global CLI command (Cisco IOS Software enables the **service dhcp** CLI command globally by default).
DHCP Relay (Subnet Broadcast)	Disabled	Enabled	Cisco IOS DHCP Relay will forward DHCP Discover packets destined to a subnet broadcast address (i.e. 192.168.1.255 /24) by default. Cisco NX-OS 5.2(1) introduced this functionality, but requires the **ip dhcp relay subnet-broacast** interface command.
Protocols Forwarded	UDP 67/68	see note	Cisco IOS Software forwards DNS, NetBIOS, Neighbor Discovery, TFTP, and Time protocols by default. They can be manually disabled if desired.

Additional Notes:

- The ARP timeout should be less than the MAC address table aging timer, so the ARP updates prevent entries from timing out of the MAC address table.
- DHCP is disabled by default in Cisco NX-OS Software. DHCP can be enabled with the **feature dchp** command.
- Cisco NX-OS Software uses the **ip dhcp relay address** interface command to relay DHCP requests, whereas Cisco IOS Software uses the **ip helper-address** command.
- The Cisco NX-OS Software has a **show ip dhcp relay address** command that is useful for verifying what interfaces have DHCP-Relay's configured. Cisco IOS Software introduced the **show ip helper-address** command in later versions of the SX software release.

Layer-3 Unicast Routing Features and Protocols

This section outlines some of the default differences related to unicast routing protocols and routing functionality such as protocol redistribution.

BGP	Cisco NX-OS	Cisco IOS	Notes
Address Families	All Disabled	All Enabled	Cisco NX-OS Software requires an address family to be configured per BGP neighbor (By default, all address families are disabled).
Auto-Summarization	Disabled	Disabled	Cisco NX-OS Software doesn't have the ability to enable auto-summarization. Later versions of the Cisco IOS Software disable auto-summarization by default (Earlier versions enable it by default).
Deterministic MED	Enabled	Disabled	Deterministic MED can be disabled in Cisco NX-OS Software using the **bestpath med non-deterministic** command under the BGP routing instance.
Distance	20 / 200 / 220	20 / 200 / 200	Administrative distance (AD) values = external / internal / local. Cisco NX-OS software defaults to 220 for local-routes as opposed to 200 in Cisco IOS Software. This can be changed in Cisco NX-OS Software using the **distance <#> <#> <#>** command under the BGP routing instance address family.
Neighbor Logging	Disabled	Enabled	Cisco NX-OS Software requires the **log-neighbor-changes** command under the routing process to log neighbor adjacency changes.
Synchronization (IGP)	Disabled	Disabled	Cisco NX-OS Software doesn't have the ability to enable synchronization (IGP). Later versions of the Cisco IOS Software disable synchronization by default (Earlier versions enable it by default).
EIGRP	**Cisco NX-OS**	**Cisco IOS**	**Notes**
# of Instances	4 (per VDC)	> 4	Cisco NX-OS Software supports 4 EIGRP instances per VDC (Multiple VRF instances can be configured under each EIGRP instance).

Auto-Summarization	Disabled	Enabled	Cisco NX-OS Software doesn't have the ability to enable auto-summarization.
ECMP	8	4	-
Protocol Support	IP	IP, IPX, Appletalk	Cisco NX-OS Software only supports the Internet Protocol (IP).
ISIS	**Cisco NX-OS**	**Cisco IOS**	**Notes**
# of Instances	4 (per VDC)	> 4	Cisco NX-OS Software supports 4 ISIS instances per VDC (Multiple VRF instances can be configured under each ISIS instance).
ECMP	8	4	-
OSPFv2	**Cisco NX-OS**	**Cisco IOS**	**Notes**
# of Instances	4 (per VDC)	> 4	Cisco NX-OS Software supports 4 OSPF instances per VDC (Multiple VRF instances can be configured under each OSPF instance).
Adjacency Logging	Disabled	Enabled	Cisco NX-OS Software requires the **log-adjacency-changes** command under the routing process to log adjacency changes.
Database Link-State-ID Selection	Longest Mask Match	Shortest Mask Match	OSPF requires unique link state ID?s when inserting routes into the OSPF database. When OSPF chooses between two routes with different masks (i.e. 192.168.1.0/24 and 192.168.1.0/32) with identical link state ID?s (i.e. 192.168.1.0) into the database with identical parameters (i.e. Advertising Router), the Cisco NX-OS Software will insert the route with the longest match (/32), whereas the Cisco IOS Software will insert the route with the shortest match (/24) into the OSPF database.
ECMP	8	4	-
LSA Group Pacing Timer	10 (seconds)	240 (seconds)	The LSA group pacing timer can be modified in Cisco NX-OS Software using the **timers lsa-group-pacing <1-1800>** OSPF command.
Redistribution (Subnets)	classless	classfull	Cisco NX-OS Software redistributes subnets by default (The CIsco IOS Software **subnets** redistribution option does not exist in Cisco NX-OS Software)
Reference Bandwidth	40,000 Mbps	100 Mbps	The reference bandwidth can be modified in Cisco NX-OS Software with the **auto-cost reference-bandwidth <1-4000000>**

			command under the OSPF process.
SPF Throttle Timers (Delay/Hold/Max)	200 / 1K / 5K (msecs)	5K / 10K / 10K (msecs)	Both Cisco NX-OS and IOS Software have OSPF commands to modify these timers.
Redistribution (Protocol)	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Direct Routes (Connected)	Disabled	Enabled	When redistributing routing protocols (i.e. OSPF into BGP or OSPF into EIGRP) directly connected routes within the source routing protocol (i.e. OSPF) are not redistributed into the target routing protocol by default in Cisco NX-OS Software. Cisco NX-OS Software requires the **redistribute direct** command under the target routing instance.
Route-Map Required	Yes	No (Optional)	Cisco NX-OS Software requires a route-map when redistributing routes between different routing protocols (i.e. OSPF to BGP) or different routing instances (i.e. OSPF 10 to OSPF 20). In Cisco NX-OS software, a configured route-map without a prefix-list will redistribute all routes by default (permit). A prefix-list can be configured (not an ACL) to select specific routes for redistribution.
RIPv2	**Cisco NX-OS**	**Cisco IOS**	**Notes**
# of Instances	4 (per VDC)	> 4	Cisco NX-OS supports 4 RIPv2 Instances per VDC (Multiple VRF instances can be configured under each RIPv2 instance).
Default-Metric	1	0	The default-metric can be modified under the RIP instance or in a route-map when performing protocol redistribution in both Cisco NX-OS and IOS Software.
ECMP	8	4	-
Static Routes	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Configuration Placement	Under the VRF instance	Global Configuration	Cisco NX-OS software requires static routes to be configured under the VRF instance, whereas Cisco IOS Software appends the **vrf** option on the global **ip route** command.

Additional Notes:

- IP classess routing is enabled by default in Cisco NX-OS Software and in later versions of Cisco IOS Software. Cisco NX-OS Software does not have a CLI command to disable it.
- IP subnet-zero is enabled by default in Cisco NX-OS Software and in later versions of Cisco IOS Software. Cisco NX-OS Software does not have a CLI command to disable it.

- All dynamic routing protocols are disabled by default in Cisco NX-OS Software. Routing protocols can be enabled with the **feature bgp**, **feature eigrp**, **feature isis**, **feature ospf**, **feature rip** commands.
- Routing parameters can be modified for both Cisco NX-OS and Cisco IOS Software, so routing protocols can operate in a consistent manner in mixed environments.
- Cisco NX-OS Software supports up to 16 ECMPs, whereas later versions of Cisco IOS Software supports up to 32.
- VRF instances are assigned to routing protocols differently in the Cisco IOS Software. Some routing protocols allow multiple VRF instances to be associated to a single process (i.e. EIGRP), whereas others require a unique process ID per VRF instance (i.e. OSPF).
- The number of routing processes varies per Cisco IOS Software release. Earlier releases supported 32 processes per system. However, that has been modified to allow a much larger number of processes to support hundreds of VRF instances.
- It is generally recommended to use the same reference-bandwidth value throughout an OSPF domain.

Multicast Features and Protocols

The following table outlines the default differences for multicast feaures and routing protocols.

IGMP	**Cisco NX-OS**	**Cisco IOS**	**Notes**
IGMP (Query Interval)	125 (seconds)	60 (seconds)	The query interval can be configured per interface in Cisco NX-OS Software with the **ip igmp query-interval <1-18000>** command.
IGMP (Query Timeout)	255 (seconds)	120 (seconds)	The query timeout can be configured per interface in Cisco NX-OS Software with the **ip igmp query-timeout <1-65535>** command.
Snooping (Lookup)	IP	MAC	Catalyst 6500's with Sup720's (EARL 7) only support MAC lookups, whereas Sup2T's (EARL 8) default to an IP lookup.
Snooping (Report-Suppression)	Enabled	Disabled	-
Snooping (V3-Report-Suppression)	Enabled	Disabled	-
PIM	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Auto-RP Candidate	Not Configured	224.0.0.0/4	Cisco NX-OS Software requires a group list to be configured when configuring the Auto-RP Candidate.
Auto-RP Forwarding	Disabled	Enabled	Cisco NX-OS Software requires the global **ip pim auto-rp forward listen** command.
Auto-RP Scope (Mapping-Agent and Candidate-RP)	32	Not Configured	Cisco IOS Software requires the scope to be configured with the **scope** option.
		Filters BSR	

Border Configuration (Filtering)	Filters BSR and Auto-RP		In Cisco NX-OS Software the **ip pim border** interface command filters both BSR and Auto-RP packets, whereas the Cisco IOS Software requires the **ip pim bsr-border** (filters BSR packets) and the **ip multicast boundary** (filters Auto-RP packets) interface commands.
BSR Candidate Priority	64	0	A higher numeric value is preferred. The priority can be modified in both Cisco NX-OS and IOS Software.
BSR Candidate-RP Group-List	Not Configured	224.0.0.0/4	Cisco NX-OS Software requires a group list to be configured when configuring the BSR Candidate-RP.
BSR Candidate-RP Priority	192	0	A lower numberic value is preferred. The priority can be modified in both Cisco NX-OS and IOS Software.
BSR Forwarding	Disabled	Enabled	Cisco NX-OS Software requires the global **ip pim bsr forward listen** command.
Load Sharing	ECMP	1 for all (*,G) & (S,G)	Cisco NX-OS Software runs a hash with source/RP addresses to select RPF interface.
Logging (Neighbor Changes)	Disabled	Enabled	PIM neighbor logging can be enabled globally in Cisco NX-OS Software with the **ip pim log-neighbor-changes** command.
Software ASM Replication	Disabled	Enabled	Cisco NX-OS Software can enable ASM software replication with the global **ip routing multicast software-replicate** command.
Source-Specific Mode (SSM)	Enabled	Disabled	SSM is configured for address range 232.0.0.0/8 in Cisco NX-OS Software by default (SSM can be disabled with the **no ip pim ssm range 232.0.0.0/8** global command. SSM is disabled in Cisco IOS Software by default.
MSDP	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Source-Active Data Cache	Enabled	Disabled	MSDP SA data caching is disabled by default in Cisco IOS Software.

Additional Notes:

- Multicast routing protocols are disabled by default in Cisco NX-OS Software . PIM and MSDP can be enabled with the **feature pim** and **feature msdp** commands (IGMP is enabled by default). Cisco IOS Software requires the global **ip multicast-routing** command to enable multicast routing.

MPLS Features and Protocols

The following table outlines the default differences for MPLS features and protocols such as LDP, L3VPN, mVPN, RSVP-TE.

		Cisco IOS	**Notes**

Label Discovery Protocol (LDP)	**Cisco NX-OS**		
Graceful Restart	Enabled	Disabled	-
Graceful Restart Fowarding Holding Time	120 (seconds)	600 (seconds)	The Cisco NX-OS LDP graceful-restart forwarding holding timer can be configured with the **graceful-restart timers forwarding-holding <30-600>** LDP command.
Label Range (min / max)	16 / 471804	16 / 100000	The Cisco NX-OS label range can be configured with the **mpls label range <16-492286>** global command.
Multicast VPN (mVPN)	**Cisco NX-OS**	**Cisco IOS**	**Notes**
MDT MTU (Tunnel MTU in bytes)	1376	1500	The MDT MTU can be modified under a VRF context using the **mdt mtu** command in Cisco NX-OS Software.

Additional Notes:

- In Cisco NX-OS, the MPLS feature set needs to be installed in the default VDC(1) with the **install feature-set mpls** configuration command. The feature set has to be enabled per VDC using the **feature-set mpls** configuration command, before the **feature mpls <ldp | l3vpn | traffic-engineering>** command(s) can be executed.
- In Cisco NX-OS, global LDP configuration parameters are configured under the **mpls ldp configuration** mode.
- In Cisco NX-OS, the global **feature mvpn** command is required to configure multicast vpn (mVPN) on a PE router.

Security Features and Protocols

This section contains default differences for security features and protocols such as ACLs, Hardware Rate-Limiters, Intrusion Detection System (IDS) Packet Checks, etc...

AAA	**Cisco NX-OS**	**Cisco IOS**	**Notes**
AAA Authentication (Default Fallback)	Local Username	Denies Access	Cisco NX-OS Software falls back to the local database, whereas Cisco IOS Software requires additional configuration options.
AAA Accounting	All Features	Requires Additional Configuration	Cisco NX-OS Software logs all EXEC and configuration commands with start/stop records when AAA accounting is configured.
AAA Accounting (Local)	Enabled	Disabled	The Cisco NX-OS Software logs CLI configuration commands locally by default in

			NVRAM (The **show accounting log** command can be used to view the contents).
Extended Access-Control-List (ACL)	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Egress ACL Processing (Egress CPU Generated Control Plane Packet Behavior)	Deny / Permit	Permit	Prior to Cisco NX-OS software 4.1(3), control plane packets generated by the CPU (i.e. HSRP, OSPF, etc.) are subject to egress ACL processing by default (when an egress ACL is applied to an interface). Therefore, the egress ACL requires permit entries configured for required CPU control plane packets. Cisco IOS Software permits CPU generated control plane packets by default when an egress ACL is applied to an interface (CPU generated control plane packets are not subject to egress ACL processing when applied to an interface). In Cisco NX-OS Software release 4.1(3) and onward, the default behavior is the same as Cisco IOS Software.
Hardware Rate Limiters	**Cisco NX-OS**	**Cisco IOS**	**Notes**
access-list-log	100 pps	N/A	Packets copied to the supervisor for access-list logging
copy	30K pps	N/A	Data and control plane packets copied to the supervisor module
f1 rl-1	4500 pps	N/A	Related to F1 module
f1 rl-2	1000 pps	N/A	Related to F1 module
f1 rl-3	1000 pps	N/A	Related to F1 module
f1 rl-4	100	N/A	Related to F1 module
f1 rl-5	1500 pps	N/A	Related to F1 module
layer-2 l2tp	500 pps	Disabled	Layer-2 Tunnel Protocol packets - New in NX-OS

			5.0
layer-2 lisp-map-cache	500 pps	N/A	-
layer-2 mcast-snooping	10K pps	Disabled	IGMP Snooping Packets
layer-2 port-security	Disabled	Disabled	Packets violating MAC restrictions on inbound interfaces
layer-2 storm-control	Disabled	N/A	Packets flooded in VLAN
layer-2 vpc-low	4K pps	N/A	Control packets over vPC low queue
layer-2 vpc-peer-gateway	5000 pps	N/A	-
layer-3 control	10K pps	N/A	Control packets
layer-3 glean	100 pps	100 pps	Packets failing RPF
layer-3 mtu	500 pps	Disabled	Packets failing MTU check
layer-3 multicast directly-connected	3k pps	Disabled	Data packets punted for ASM source registration
layer-3 multicast local-groups	3K pps	N/A	Data packets punted for initializing SPT join
layer-3 multicast rpf-leak	500 pps	Disabled	Packets failing RPF
layer-3 ttl	500 pps	Disabled	Packets failing TTL check
receive	30K pps	Disabled	Packets redirected to the supervisor
IDS Packet Checks (IPv4)	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Address Source Broadcast	Enabled	N/A	Source IP Address is 255.255.255.255
Address Source Multicast	Enabled	N/A	Source IP Address is 224.x.x.x
Address Destination Zero	Enabled	N/A	Destination IP Address is 0.0.0.0
Address Identical	Disabled	N/A	Same Source and Destination IP Address
Address Reserved	Disabled	N/A	Source IP address is 127.0.0.0
Address Class-E	Disabled	N/A	Reserved address range (240.0.0.0 - 255.255.255.255)
Checksum	Enabled	N/A	Verify IPv4 and IPv6 packet checksum
Protocol	Enabled	N/A	Verify IP protocol
Fragment	Disabled	N/A	Check IPv4 and IPv6 fragment with non-zero offset and the DF bit set

Length Minimum	Enabled	N/A	Validate IPv4 packet header and payload length - Minimum IPv4 header length
Length Consistent	Enabled	N/A	Validate IPv4 packet header and payload length - Actual frame size is equal too or more than IPv4 length plus Ethernet header
length maximum max-frag	Enabled	N/A	Validate IPv4 packet header and payload length - Fragment offset field value
Length Maximum UDP	Disabled	N/A	-
Length Maximum Max-TCP	Enabled	N/A	Validate IPv4 packet header and payload length - Maximum TCP length has to be less than the IPV4 payload length
TCP Flags	Disabled	N/A	-
TCP Tiny-Frag	Enabled	N/A	Validate TCP Header - Check TCP tiny fragment
Version	Enabled	N/A	Must be version 4 for an Ethertype (0x0800)
RADIUS	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Vendor Specific Attributes (VSA)	Enabled	Disabled	Cisco IOS Software requires the global **radius-server send vsa** command.

Additional Notes:

- Prior to Cisco NX-OS Software 4.(1)3, the default can be modified to permit control plane packets originated from the CPU with the **ip access-list match-local-traffic** global command.
- Cisco NX-OS Software hardware rate-limiter status and statistics can be verified using the **show hardware rate-limiters** command.
- Cisco NX-OS Software Intrusion Detection System (IDS) packet check status and statistics can be verified using the **show hardware forwarding ip verify** command.

Quality of Service Features

This section contains default differences for Quality of Service (QoS) features.

QoS (General)	**Cisco NX-OS**	**Cisco IOS**	**Notes**
	Enabled	Disabled	

Global Configuration			Cisco IOS Software requires the global **mls qos** command to enable QoS.
Interface Trust State	Trusted	Untrusted	In Cisco NX-OS Software, all CoS(L2) / DSCP(L3) / ToS(L3) marking are preserved (A QoS policy can be configured to rewrite the values). In CIsco IOS Software all ports are untrusted by default, so the CoS(L2) / DSCP (L3) / ToS(L3) markings are cleared by default when QoS is enabled.

Additional Notes:

- The Cisco IOS Software default QoS behavior can be modified with the **no mls rewrite dscp** global command to preserve the CoS/ToS/DSCP markings.
- If the Cisco IOS Software is configured with the **mls qos queuing-only** command, the CoS/ToS/DSCP markings are preserved.
- In Cisco NX-OS Software, control plane packets generated by the CPU are not subject to egress interface QoS processing even though QoS is enabled by default. In Cisco IOS Software, control plane packets generated by the CPU are subject to egress QoS policies when QoS is enabled with the global **mls qos** command.

Network Management Features and Protocols

This section contains default differences for network management features and protocols.

NetFlow	**Cisco NX-OS**	**Cisco IOS**	**Notes**
Export Port (NDE)	UDP 9995	None	In Cisco NX-OS Software, the destination UDP port for the NDE packet does not need to be specified (UDP 9995 is the default). However, a different UDP port can be specified with the flow exporter **transport udp <1 - 65535>** command.
Export Version	5	1	Both CIsco NX-OS and IOS Support versions 5 and 9, which are the most commonly deployed.
Multicast Statistics Collection	Enabled	Disabled	The Cisco IOS Software requires the global **ip multicast netflow output-counters** command.
Sampling (Packet Based)	1-64 out of 1-8192	64-8192 out of 8K-16K	NetFlow Sampling is disabled by default in both Cisco NX-OS and IOS Software. However, when configuring packet based sampling, the sample packet rates are different. Cisco NX-OS software allows any value with the configurable range, whereas Cisco IOS Software requires packet increments 64, 128, 256 up to 8192 to be specified.
Timer (Active Aging)	1800 (seconds)	1920 (seconds)	-
Timer (Fast Aging)	32 - 512 (seconds)	32	Fast Aging is disabled by default in both CIsco NX-OS and IOS Software. However, Cisco NX-OS requires a value when configuring it, wherase the Cisco IOS defaults to 32 seconds and supports a range between <1-128>.
Timer	15	256	-

(Inactive Aging)	(seconds)	(seconds)	
SNMP	**Cisco NX-OS**	**CIsco IOS**	**Notes**
Interface Persistance	Enabled	Disabled	Interface persistance is enabled by default and cannot be disabled in Cisco NX-OS Software. Cisco IOS Software requires the global**snmp-server ifindex persist** command.
Users (SNMPv3)	admin	None	Cisco NX-OS Software automatically creates a SNMPv3 user account by default when a local user is created with the **username** command. The snmp user account is displayed in the configuration with the **snmp-server user** global command. By default, the **admin** SNMP user account is configured.

Additional Notes:

- NetFlow is disabled by default in Cisco NX-OS Software (NetFlow can be enabled with the global **feature netflow** command).