Unicast routing features

Unicast routing features are a comprehensive suite of protocols, mechanisms, and services responsible for determining the optimal path and forwarding IP packets from a single source to a single, specific destination across one or more interconnected networks. Their primary function is to build and maintain a routing table that enables intelligent, hop-by-hop packet delivery.

Starting with Cisco NX-OS Release 10.6(1s), you can configure these unicast routing features on the Cisco N9324C-SE1U, Cisco N9348Y2C6D-SE1U switches.

Core IP services and addressing

These are the fundamental protocols and concepts required for basic IP communication on a local network segment.

- **IPv4/IPv6 unicast routing**is the fundamental process of forwarding IP packets from a single source device to a single, specific destination device using their unique IPv4 or IPv6 addresses. Layer 3 uses either the IPv4 or IPv6 protocol. IPv6 increases the number of network address bits from 32 bits (in IPv4) to 128 bits.

  For more information on IPv4 Unicast routing, see IPv4 addresses.

  For more information on IPv6 Unicast routing, see Configuring IPv6.

- **Host route** is a specific type of route in a routing table that directs traffic to a single host IP address using a /32 (for IPv4) or /128 (for IPv6) prefix length.

  For more information on host route, see IPv4 addresses and Configuring IPv6.

- **Address Resolution Protocol (ARP)** is a protocol used to map a known IPv4 address to its corresponding Layer 2 MAC address within a local network segment.

  For more information on host route, see IPv4 addresses and Configuring IPv6.

- **Neighbor Discovery (ND)** is an IPv6 protocol suite that replaces ARP and provides additional functions such as router discovery, address autoconfiguration, and neighbor reachability tracking.

  For more information on host route, see IPv4 addresses and Configuring IPv6.

Routing protocols

These are the dynamic protocols used to build and maintain routing tables by exchanging reachability information with other routers.

- **Border Gateway Protocol (BGP)**is an inter-autonomous system routing protocol. A BGP router advertises network reachability information to other BGP routers using Transmission Control Protocol (TCP) as its reliable transport mechanism. The network reachability information includes the destination network prefix, a list of autonomous systems that needs to be traversed to reach the destination, and the next-hop router. Reachability information contains additional path attributes such as preference to a route, origin of the route, community and others.

  For more information on BGP, see Configuring BGP.

- **Open Shortest Path First (OSPF)** protocol is a link-state routing protocol used to exchange network reachability information within an autonomous system. Each OSPF router advertises information about its active links to its neighbor routers. Link information consists of the link type, the link metric, and the neighbor router that is connected to the link. The advertisements that contain this link information are called link-state advertisements. For more information on OSPF, see Configuring OSPFv2.

- **Intermediate System-to-Intermediate System (IS-IS)** protocol is an intradomain Open System Interconnection (OSI) dynamic routing protocol specified in the International Organization for Standardization (ISO) 10589. The IS-IS routing protocol is a link-state protocol. IS-IS features are as follows:

  - Hierarchical routing
  - Classless behavior
  - Rapid flooding of new information
  - Fast Convergence
  - Very scalable

  For more information on ISIS, see Configuring IS-IS.

Traffic forwarding and path control

These features influence how a router forwards packets based on the information in its routing table.

- **Equal-Cost Multi-Path (ECMP)** is a routing mechanism that allows a device to load-balance traffic across multiple paths when they all have the same routing cost to a given destination.

  For more information on ECMP, see Overview.

- **IP Directed Broadcast** is a feature that enables a packet, addressed to the broadcast IP of a remote subnet, to be routed as a unicast packet across the network until the final router translates it into a local Layer 2 broadcast on the destination segment.

  For more information on IP directed broadcast, see Configuring IP Directed Broadcasts.

- **Policy-Based Routing (PBR)** is a feature that enables a network device to override its standard destination-based routing table for specific traffic flows. By using policies, typically defined by an access list, to classify unicast packets based on criteria like source/destination IP, protocol, or port number, PBR can redirect that traffic to a designated next-hop IP address or egress interface, allowing for customized traffic paths for purposes like service chaining or traffic engineering.

  For more information on IP directed broadcast, see Configuring Policy-Based Routing.

Security features

These features are designed to protect the network from common Layer 3 attacks.

- **Unicast Reverse Path Forwarding (uRPF)** is a security feature that helps prevent IP address spoofing by verifying that the source IP address of an incoming packet is reachable through the same interface on which the packet was received.

  For more information on IP directed broadcast, see Configuring HSRP.

Interface configuration features

This category includes specialized ways to configure IP on an interface.

- **IP Unnumbered (non-SVI) interface** is a feature that enables a point-to-point physical interface (non-SVI) to process IP traffic without having its own assigned IP address, typically by "borrowing" the IP address from another interface.

  For more information on non SVI IP unnumbered interface, see IPv4 addresses and Configuring IPv6.

High Availability and redundancy

This category includes features designed to prevent single points of failure, provide resilient network paths, and ensure continuous operation.

- **Hot Standby Router Protocol (HSRP)** is a first-hop redundancy protocol (FHRP) that provides transparent, high-availability gateway services for IP hosts. It achieves this by creating a virtual router, with a shared virtual IP and virtual MAC address, from a group of physical routers. Within the group, one router is elected as the **active** router to forward traffic, while another becomes the **standby** router, ready to take over instantly if the active router fails.
- **Virtual Router Redundancy Protocol (VRRP)** allows for a transparent failover at the first-hop IP router by configuring a group of routers to share a virtual IP address. VRRP selects an allowed router in that group to handle all packets for the virtual IP address. The remaining routers are in standby and take over if the allowed router fails.

  For more information on VRRP, see Configuring VRRP.
- **Virtual Port-Channel (vPC)** is a virtualization technology that allows two physical network switches to appear as a single logical switch to a connected device, enabling all-active link aggregation for increased bandwidth, providing high availability, and creating a loop-free topology.
- **vPC Peer Gateway** is a feature that allows a vPC switch to act as the active gateway for packets addressed to the shared router MAC address, enabling local forwarding of traffic without sending it across the vPC peer-link, which optimizes routing and improves compatibility with network-attached storage (NAS) devices.

For more information on HSRP, vPC, and vPC peer gateway, see Configuring HSRP.

Layer 2 addressing and interface configuration

This category includes features related to the configuration and management of Layer 2 addresses and interface properties.

- **User-defined MAC address** is a manually configured Layer 2 address that overrides the default hardware address for a logical interface, such as a Switched Virtual Interface (SVI) or a vPC system, to ensure a stable and predictable identity in the network.

  For more information on user-defined MAC address, see Configuring HSRP.

- Unicast routing feature guidelines, on page 4

Unicast routing feature guidelines

This section outlines feature support, guidelines, and limitations for unicast routing functionalities on Cisco N9324C-SE1U, Cisco N9348Y2C6D-SE1U switches.

Table 1: Supported features and releases

Features	Release
IPv4 Layer-3 features • **IPv4 unicast routes** • **IPv4 host routes** • **IPv4 Neighbor Discovery** • **ARP** • **IP directed broadcast** • **Non SVI IP unnumbered interface**	10.6(1s)
IPv6 Layer-3 features • **IPv6 unicast routes** • **IPv6 host routes** • **IPv6 Neighbor Discovery** • **ARP**	10.6(1s)
BGP	10.6(1s)
ECMP	10.6(1s)
OSPFv2 and OSPFv3	10.6(1s)
OSPFv2	10.6(1s)
IS-IS	10.6(1s)
Policy-based routing	10.6(1s)
uRPF	10.6(1s)
HSRP	10.6(1s)

Features	Release
VRRP	10.6(1s)
vPC and vPC peer gateway	10.6(1s)
User-defined MAC address	10.6(1s)

Supported PBR features:

- Base redirection
- 32 way ECMP
- NULL routes
- IPv4 and IPv6 PBR policies

Supported PBR features:

- Default next hop
- Set VRF
- Fast convergence
- MPLS
- SRTE
- VXLAN
- Tunnel support

User-defined MAC address limitations:

- For Cisco N9324C-SE1U, Cisco N9348Y2C6D-SE1U switches, of the total Router MAC scale, the number of unique 32 bit MSBs allowed for user-defined MAC addresses is 11.