Cloud Native BNG User Plane Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.4.x

First Published: 2021-07-01

Last Modified: 2022-02-01

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

Note This product has reached end-of-life status. For more information, see the End-of-Life and End-of-Sale Notices.

The Cisco IOS XR Software Release 7.3.1 introduces the support for cloud native broadband network gateway (cnBNG) user plane for the Cisco IOS XR platform. cnBNG is an architectural evolution that is based on Control and User Plane Separation (CUPS), where the control plane (CP) and user plane (UP) run in distinct and independent environments. This book describes the cnBNG user plane functionality and related configurations on Cisco ASR 9000 Series Routers.

For details on the commands related to the cnBNG user plane, see the Cloud Native Broadband Network Gateway User Plane Command Reference for Cisco ASR 9000 Series Routers.

For details on cnBNG deployment, the control plane functionality and the related configurations, see the *Cloud Native Broadband Network Gateway Control Plane Configuration Guide*.

To know more about physical BNG on the Cisco IOS XR platform, see the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

This preface contains these sections:

Changes to This Document

Date	Summary
February 2022	Republished for Release 7.4.2.
July 2021	Initial release of this document.

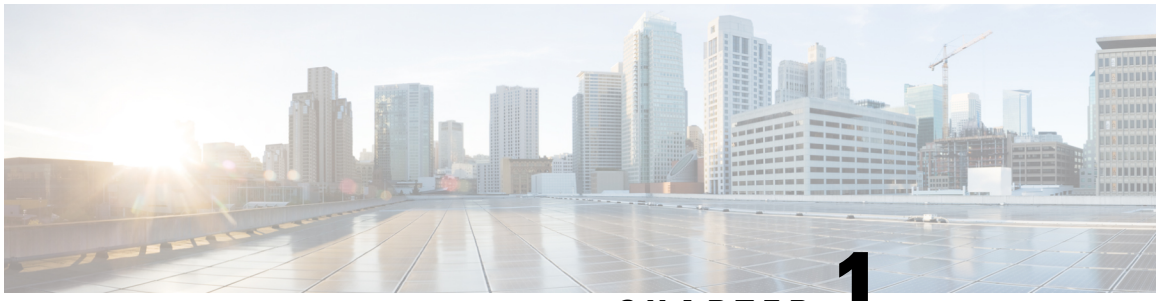
Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

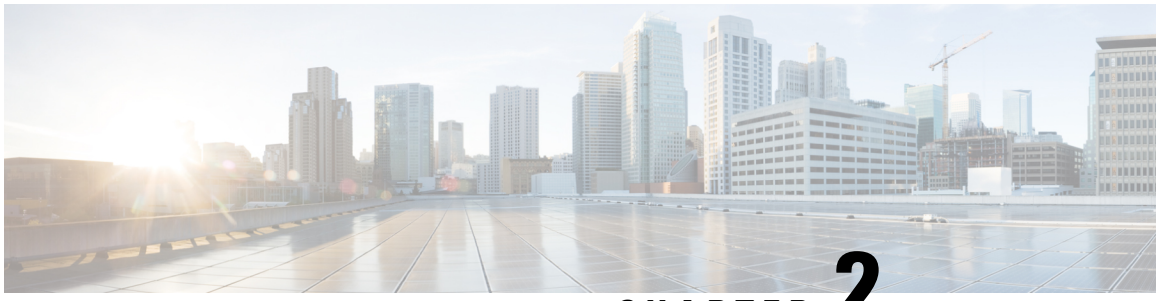
New and Changed Cloud Native BNG User Plane Features

This table summarizes the new and changed feature information for the *Cloud Native BNG User Plane Configuration Guide for Cisco ASR 9000 Series Routers*, and tells you where they are documented.

Cloud Native BNG User Plane Features Added or Modified in IOS XR Release 7.4.x

Feature	Description	Changed in Release	Where Documented
End-to-End Flow Control	This feature was introduced	Release 7.4.2	End-to-End Flow Control, on page 66
Disable Notifications for Dynamic Programming of Subscriber Gateway Address	This feature was introduced	Release 7.4.2	Configure Subscriber Gateway Address and Subnet Route, on page 32
Enable LAC on Cloud Native BNG	This feature was introduced	Release 7.4.2	L2TP Access Concentrator Sessions (LAC), on page 57
Enable LNS on Cloud Native BNG	This feature was introduced	Release 7.4.2	L2TP Network Server Sessions (LNS), on page 61
Establishing Cloud Native BNG Sessions over Pseudowire Headend (PWHE)	This feature was introduced	Release 7.4.2	Configure Cloud Native BNG over Pseudowire Headend, on page 37

Feature	Description	Changed in Release	Where Documented
Increased Granularity for Cloud Native BNG Traffic Management with Hierarchical QoS (H-QOS)	This feature was introduced	Release 7.4.2	Subscriber Features, on page 19
Multiple Framed IPv4 and IPv6 Routes for Customer Premises Equipment (CPE)	This feature was introduced	Release 7.4.2	Subscriber Features, on page 19
Cloud Native BNG feature extension to 5th Generation Line Card	This feature was introduced	Release 7.4.2	Subscriber Features, on page 19
No new features	NA	Release 7.4.1	NA



CHAPTER 2

Cloud Native BNG Overview

The Cloud Native Broadband Network Gateway (cnBNG) redefines the traditional physical BNG by decoupling the subscriber management and forwarding functions of the control plane (CP) and user plane (UP) to give better flexibility and scalability for the service providers. The cnBNG architecture is based on Control and User Plane Separation (CUPS), where the CP performs the policy and charging rule function (PCRF), whereas the UP performs policy enforcement function (PEF) of the overall BNG subscriber management solution. The cnBNG solution provides optimum scale dimensioning in terms of the number of subscriber sessions and forwarding capacity and aims at rapid deployment of multi-access services for the users. It also acts as a step forward towards converging the fixed line and mobile networks at all network layers.

Overview

The Broadband Network Gateway (BNG) is the access point for subscribers, through which they connect to the broadband network. When a connection is established between BNG and Customer Premise Equipment (CPE), the subscriber can access the broadband services provided by the Network Service Provider (NSP) or Internet Service Provider (ISP).

BNG establishes and manages subscriber sessions. When a session is active, BNG aggregates traffic from various subscriber sessions from an access network, and routes it to the network of the service provider.

BNG is deployed by the service provider and is present at the first aggregation point in the network, such as the edge router. An edge router, like the Cisco ASR 9000 Series Router, needs to be configured to act as the BNG. Because the subscriber directly connects to the edge router, BNG effectively manages subscriber access, and subscriber management functions such as:

- Authentication, Authorization, and Accounting (AAA) of subscriber sessions
- Address assignment
- Security
- Policy management
- Quality of Service (QoS)

Implementing the BNG provides the following benefits:

- Communicates with authentication, authorization, and accounting (AAA) server to perform session management and billing functions besides the routing function. This feature makes the BNG solution more comprehensive.
- Provides different network services to the subscriber. This enables the service provider to customize the broadband package for each customer based on their needs.

Cisco provides two BNG solutions:

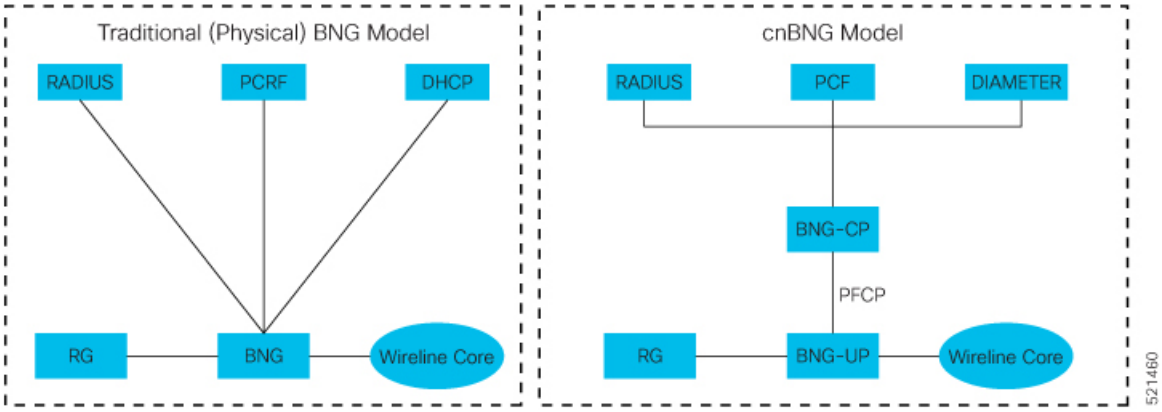
- **Physical BNG** where the BNG Control Plane (CP) and the User Plane (UP) are tightly coupled inside a Cisco IOS XR platform where the CP runs on an x86 CPU and the UP runs on a physical NPU or ASIC.

  For more information about the physical BNG, refer to the latest version of the *Broadband Network Gateway Configuration Guide* for Cisco ASR 9000 Series Routers.
- **Virtual BNG (vBNG)** where the BNG CP and UP run in separate VM-based Cisco IOS XR software on general purpose x86 UCS servers.

Evolution of cnBNG

The Cisco Cloud Native Broadband Network Gateway (cnBNG) provides a new dimension to the Control Plane and User Plane Separation (CUPS) architecture of the Broadband Network Gateway (BNG), enabling flexibility and rapid scaling for Internet Service Providers (ISPs).

Figure 1: Evolution of BNG to cnBNG



The architectural change is an evolution from an integrated traditional BNG running on a single router to a disaggregated solution, where the centralized subscriber management runs on an elastic and scalable Cloud Native Control Plane (CP) and the User Plane (UP) delivers the forwarding functionality.

cnBNG Architecture

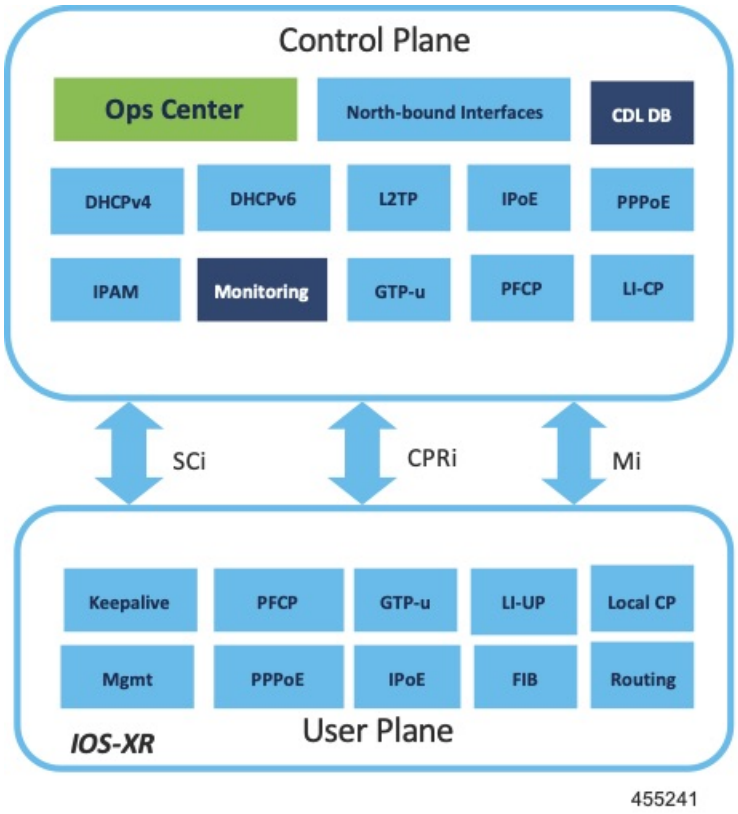
In the cnBNG architecture, the CPs and UPs are clearly and cleanly separated from each other and run in completely distinct and independent environments.

The BNG CP is moved out to a container-based microservice cloud environment.

The UP can be on any of the physical platforms that supports the BNG UP, like Cisco ASR 9000 Series Routers.

The following figure illustrates the overall cnBNG architecture.

Figure 2: cnBNG Architecture



Features and Benefits

The cnBNG supports the following features:

- **Path to convergence**: With shared Subscriber Management infrastructure, common microservices across the policy layer and shared UPs for BNG and Mobile back-haul, cnBNG paves the way for real Fixed Mobile Convergence (FMC).
- **Flexibility of scaling**: cnBNG architecture provides flexibility by decoupling the required scalability dimensions. The CP can be scaled with requirement of number of subscribers to be managed and UPs can be augmented based on the bandwidth requirements. Instead of building the CP for peak usage, the orchestrator can be triggered to deploy the relevant microservices as needed to handle the increased rate of transactions.
- **Distributed UPs**: With reduced operational complexity and minimal integration efforts with centralize CP, UPs can be distributed, closer to end-users to offload traffic to nearest peering points and CDNs. This feature reduces the core transport costs.
- **Cost effective and Leaner User planes**: With the subscriber management functions moved to cloud, you can choose cost-effective UP models for optimized deployment requirements.

The benefits of the cnBNG architecture are:

- Simplified and unified BNG CP
- Platform independent and Network Operation System (NOS) agnostic BNG CP
- Unified Policy interface across both BNG and mobility
- Common infrastructure across wireline and mobility
- Seamless migration from existing deployments
- Leverage the common infrastructure across access technologies
- Standardized model driven interface with the UP
- Data externalization for North-bound interfaces (NBI)
- Highly available and fault tolerant
- Simplified Subscriber Geo redundancy
- Horizontally scalable CP
- Independent CP and UP upgrades
- Feature agility with CI and CD
- Manageability and Operational Simplification

cnBNG Components

The cnBNG solution comprises of the following components:

Subscriber Microservices Infrastructure

The Cisco Ultra Cloud Core Subscriber Microservices Infrastructure (SMI) is a layered stack of cloud technologies that enable the rapid deployment, and seamless life-cycle operations for microservices-based applications.

The SMI stack consists of the following:

- SMI Cluster Manager—Creates the Kubernetes (K8s) cluster, creates the software repository, and provides ongoing LCM for the cluster including deployment, upgrades, and expansion.
- Kubernetes Management—Includes the K8s master and etcd functions, which provide LCM for the NF applications deployed in the cluster. This component also provides cluster health monitoring and resources scheduling.
- Common Execution Environment (CEE)—Provides common utilities and OAM functionalities for Cisco cloud native NFs and applications, including licensing and entitlement functions, configuration management, telemetry and alarm visualization, logging management, and troubleshooting utilities. Additionally, it provides consistent interaction and experience for all customer touch points and integration points in relation to these tools and deployed applications.
- Common Data Layer (CDL)—Provides a high performance, low latency, stateful data store, designed specifically for 5G and subscriber applications. This next generation data store offers HA in local or geo-redundant deployments.

- Service Mesh—Provides sophisticated message routing between application containers, enabling managed interconnectivity, additional security, and the ability to deploy new code and new configurations in low risk manner.
- NB Streaming—Provides Northbound Data Streaming service for billing and charging systems.
- NF/Application Worker nodes—The containers that comprise an NF application pod.
- NF/Application Endpoints (EPs)—The NF's/application's interfaces to other entities on the network.
- Application Programming Interfaces (APIs)—SMI provides various APIs for deployment, configuration, and management automation.

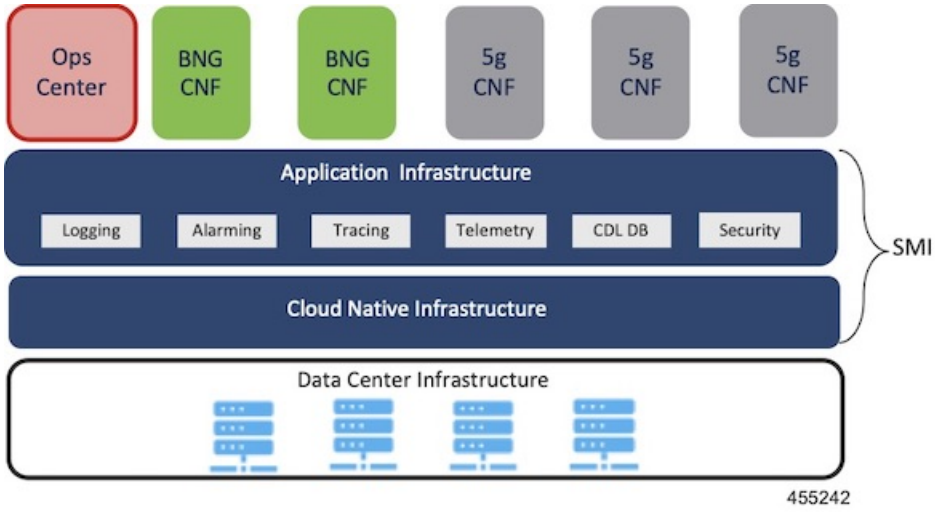
For more information on SMI components, refer to the "Overview" chapter of the *Ultra Cloud Core Subscriber Microservices Infrastructure* documentation—*Deployment Guide*.

For information on the Cisco Ultra Cloud Core, see https://www.cisco.com/c/en/us/products/collateral/wireless/packet-core/datasheet-c78-744630.html.

cnBNG Control Plane

The Cisco cnBNG CP is built on Cisco® Cloud Native Infrastructure, which is a Kubernetes-based platform that provides a common execution environment for container-based applications. This CP is built on principles of stateless microservices, to scale at-ease, introduce services much faster and more cost-effective.

Figure 3: cnBNG Control Plane Architecture



The CP runs as a Virtual Machine (VM) to adapt to existing service provider-deployed virtual infrastructure. It is built ground-up on a clean-slate architecture with a view on ‘Converged Subscriber Services’ and is aligned to 3gpp and BBF standards.

The cnBNG CP effectively manages the subscriber management functions such as:

- Authentication, authorization, and accounting of subscriber sessions
- IP Address assignment
- In-built DHCP Server

- Security
- Policy management
- Quality of Service (QoS)

Service providers can choose from wide choice of available ASR 9000 form factors, based on exact deployment requirements. The CUPS architecture allows to run these UPs in a distributed mode, to the edge of network, for early traffic offloads.

For more information about the cnBNG control plane, refer to the *Cloud Native Broadband Network Gateway Control Plane Configuration Guide.*

cnBNG User Plane

The UP delivers the forwarding functionality of the entire cnBNG solution. With the CP handling the subscriber management functionality, the cnBNG architecture enables the UP to be more distributed and interoperable with cnBNG CP with minimal integration efforts. The cnBNG Subscriber Provisioning Agent (SPA), which is the common interface between UP and CP, is bundled with the existing Cisco IOS XR image to transform an integrated physical BNG router to a cnBNG user plane.

For more information about the cnBNG UP, see the *Cloud Native BNG User Plane Overview* chapter.

License Information

cnBNG supports the following licenses:

License	Description
Application Base	Per cluster
Session (Increments)	Network-wide

These are the software license PIDs for cnBNG:

Cisco cnBNG Control Plane:

Product IDs	Description
CN-BNG-BASE-L	Base PID for cnBNG Control Plane (per cluster)
CN-BNG-100k-L	Session scale for 100,000 subscribers (network-wide) base licenses
CN-BNG-400k-L	Session scale for 400,000 subscribers (network-wide) base licenses
CN-BNG-1M-L	Session scale for 1,000,000 subscribers (network-wide) base licenses
CN-BNG-2M-L	Session scale for 2,000,000 subscribers (network-wide) base licenses

Cisco cnBNG User Planes:

Refer the ASR9000 data sheet for ordering information:
https://www.cisco.com/c/en/us/products/routers/asr-9000-series-aggregation-services-routers/datasheet-listing.html

Standard Compliance

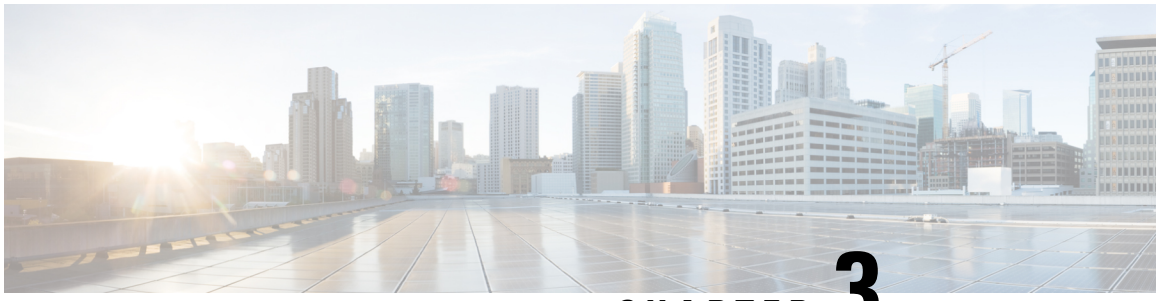
cnBNG solution is aligned with the following standard:

TR-459 Control and User Plane Separation for a disaggregated BNG

Limitations and Restrictions

The cnBNG has the following limitations and restrictions in this release:

- High availability on CP is not supported.
- Only one subnet is supported per VRF.
- QoS provisioning is supported only through service.



CHAPTER 3

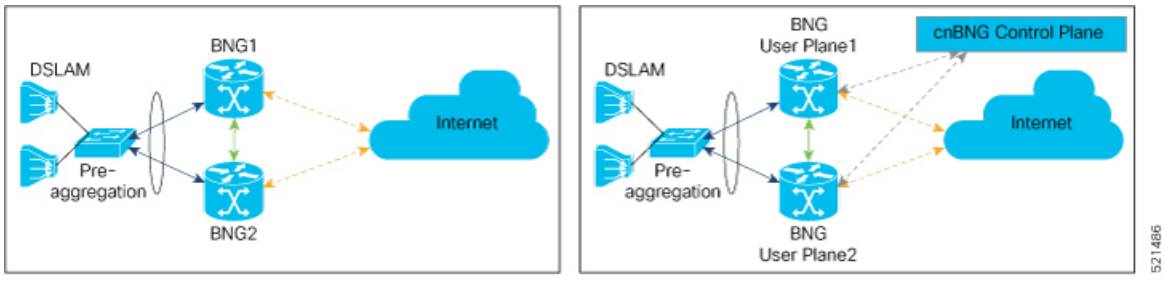
Cloud Native BNG User Plane Overview

In the cnBNG architecture, which is based on Control and User Plane Separation (CUPS), the CP handles the subscriber management functionality and the UP handles the forwarding functionality of the entire BNG solution. This chapter focuses on the functionality and architecture of the cnBNG user plane.

For more details on the cnBNG control plane, see the *Cloud Native Broadband Network Gateway Control Plane Configuration Guide*.

Control and User Plane Separation

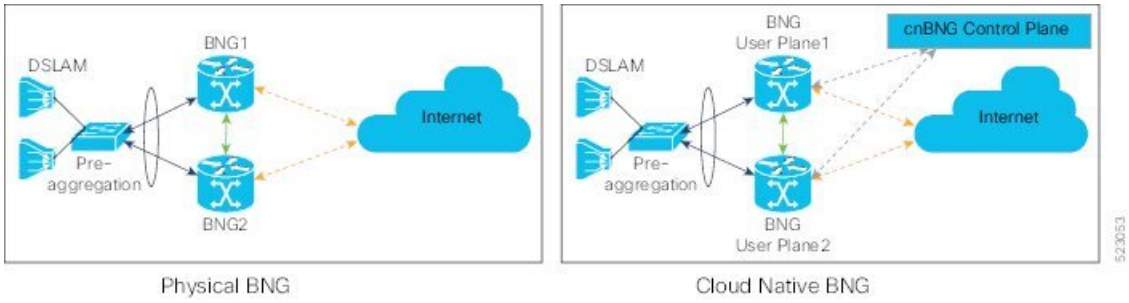
cnBNG is an architectural evolution that is based on Control and User Plane Separation (CUPS), where the CP and UP run in distinct and independent environments. cnBNG redefines the traditional physical BNG by decoupling the BNG CP and UP functions to give better flexibility and scalability for the service providers. In cnBNG, the centralized subscriber management functionality of BNG runs on CP infrastructure and the user plane delivers the forwarding functionality.



Physical BNG

Cloud Native BNG

Figure 4: Eps



In Cisco cnBNG solution, a physical Cisco IOS XR platform like Cisco ASR 9000 Series Routers provides the UP functionality. Whereas Cisco Ultra Cloud Core Subscriber Microservices Infrastructure (SMI)—a container-based microservice cloud environment, provides the CP functionality.

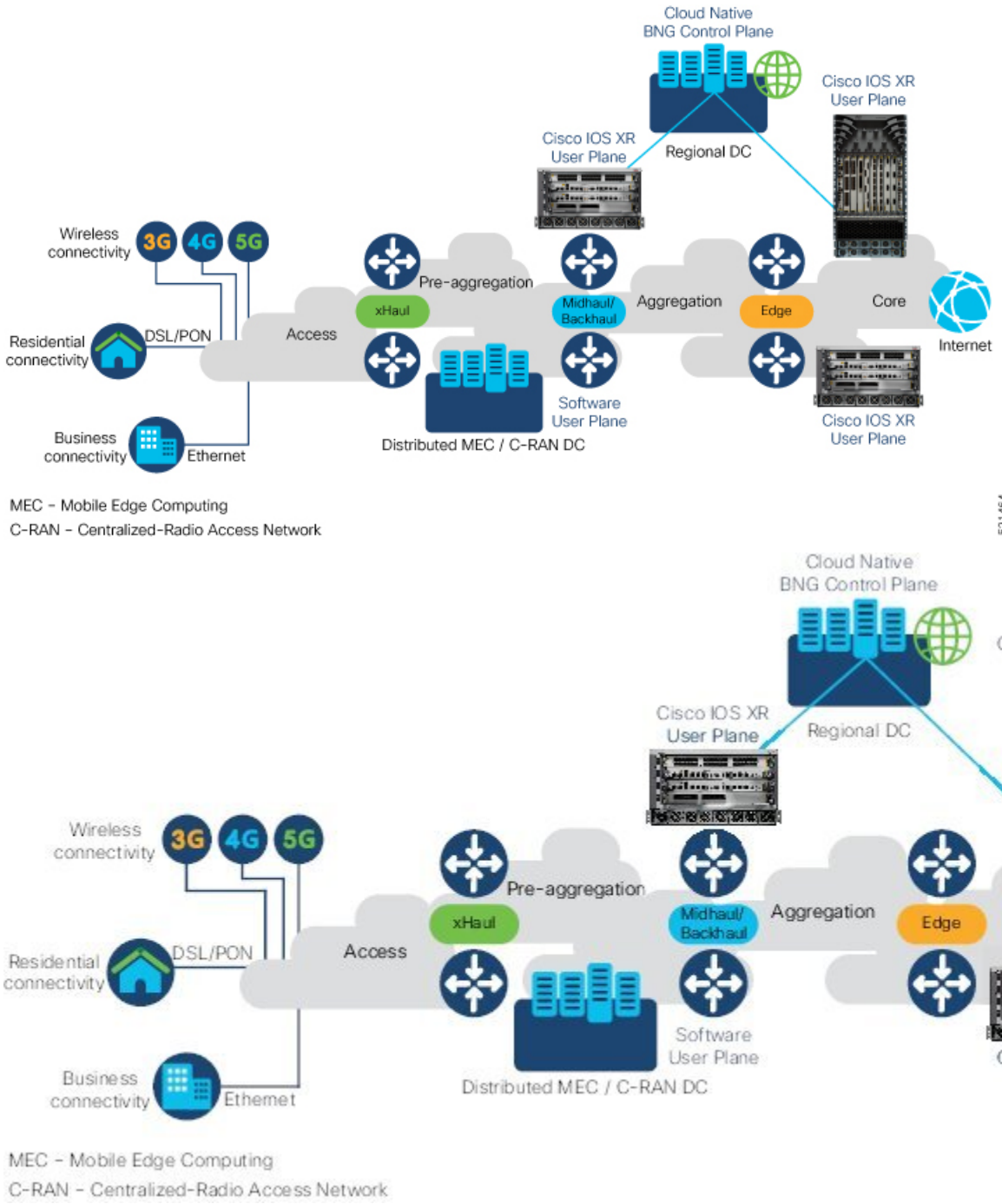
Why CUPS?

CUPS provides the capability to independently scale the CP and UP in an efficient and dynamic manner. CUPS enables network operators to optimize data center costs by hosting the CP and UP in different geographic locations. CUPS thus saves on backhaul (the access to core connection) costs by terminating data at the edge of the network. The network operators can then easily adapt to the evolving demands of mobile networks without incurring extra capital expenditures (CapEx) and operating expenditures (OpEx). The CUPS solution thus promotes a more cost-effective approach to core mobile architecture and future-proofs the network for 5G.

cnBNG User Plane Overview

Sample Network Topology for Cloud Native BNG using CUPS

Figure 5: EPS



In cloud native BNG (cnBNG), the CP provides the service policies that are sourced from the north-bound systems such as the RADIUS server or the policy and charging rules function (PCRF) node. Whereas the UP performs policy enforcement function (PEF) of the overall BNG subscriber management solution. The BNG CP protocols: RADIUS, DHCPv4, DHCPv6, PPPoE, PPP, and IP address pool management run on the CP. Whereas the non-BNG-specific protocols: IPv6 neighbor discovery (ND), ARP, routing protocols (like ISIS or BGP) that export subscriber subnet routes, and UDP or IP protocols that transport DHCPv4 or DHCPv6 payloads run on the UP.

The cnBNG UP models each subscriber as a unique flow. The system applies the subscriber features like quality of service (QoS), Hierarchial Quality of Service (HQoS),access control list (ACL), policy-based routing (PBR), lawful intercept (LI), accounting, and so on, on this flow. The DHCPv4, DHCPv6, PPPoE, and PPP protocols trigger the BNG subscriber flow. The UP presents these protocol packets to the cnBNG CP for authentication and authorization, and for evaluating policy and charging rules. Once the subscriber is accepted, the UP creates the subscriber flow and applies features on this flow. The subscriber flow can also have multiple sub-flows, and you can apply specific features to these sub-flows.

Key Features and Benefits of cnBNG User Plane

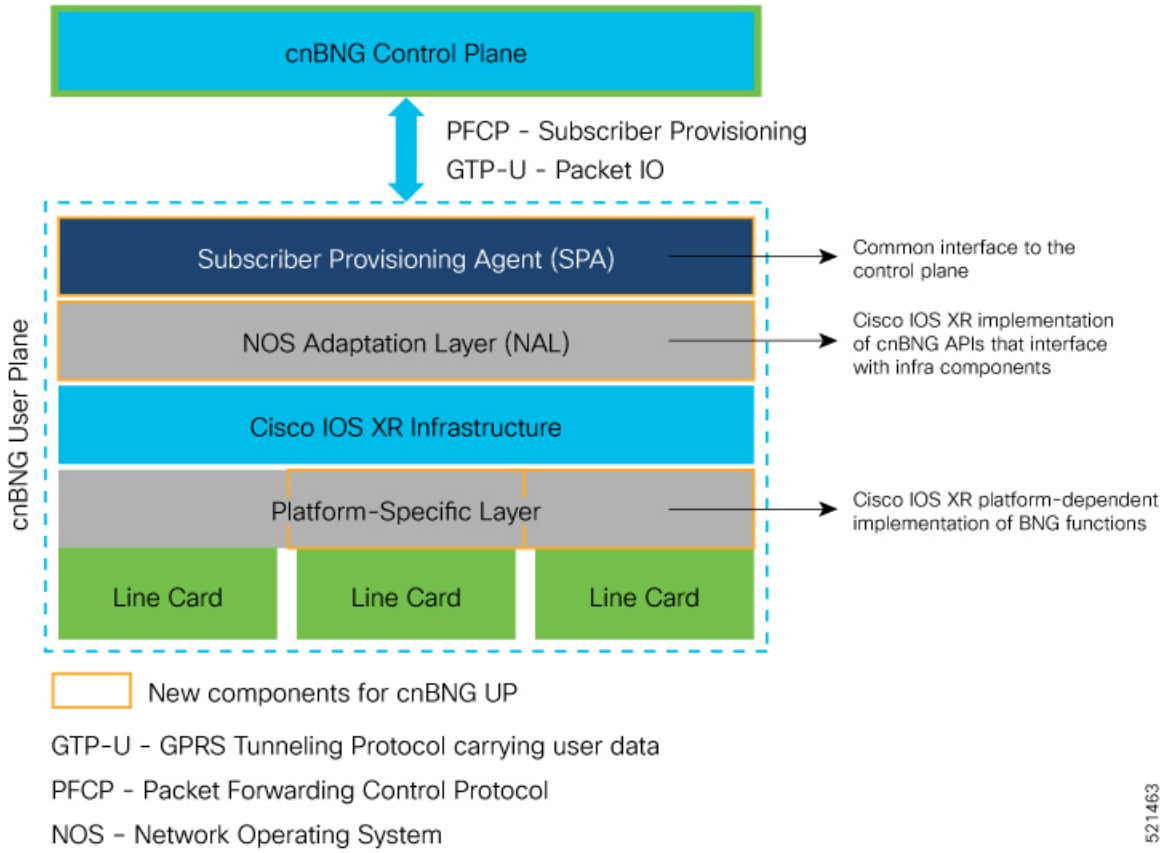
The key features and benefits of the cnBNG user plane are:

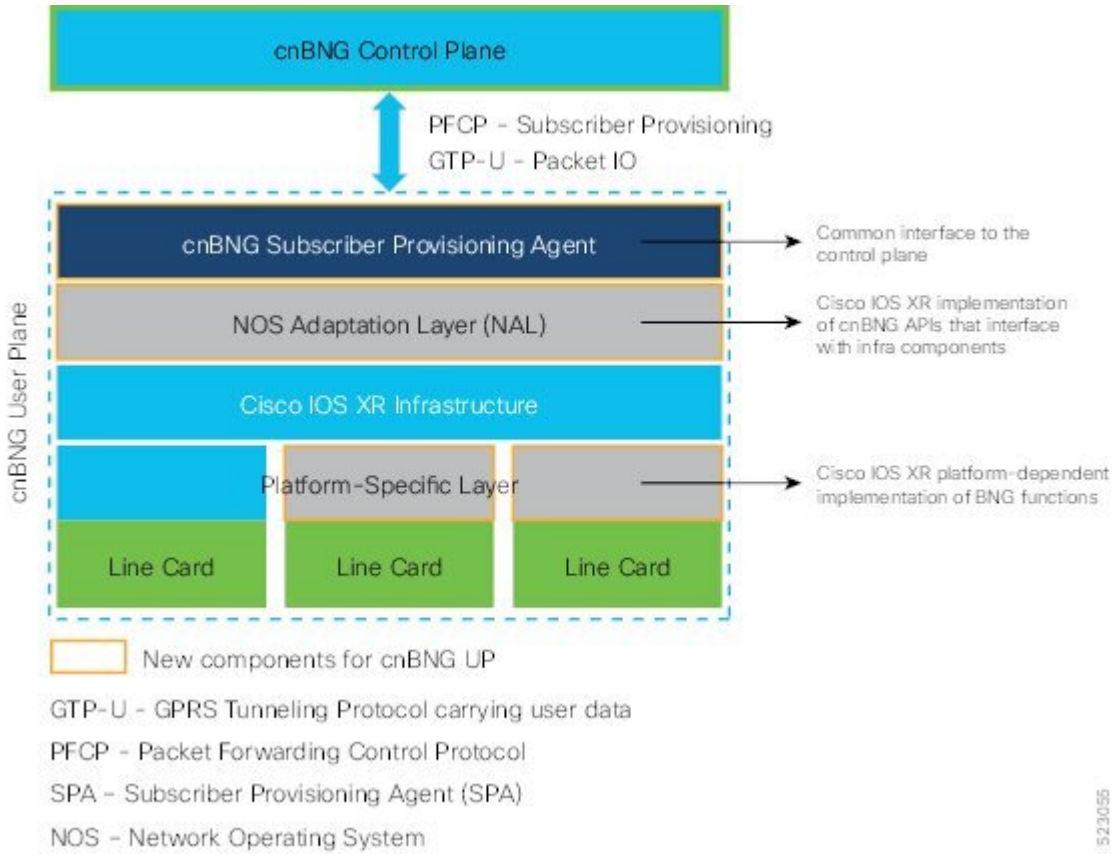
- **Distributed**: With reduced operational complexity and minimal integration efforts with centralized CP, you can distribute the UPs closer to end users. This feature helps to offload the traffic to the nearest peering points and content delivery networks (CDNs) and reduces the core transport costs.
- **Cost-effective and leaner**: With the subscriber management functions moved to cloud, you can choose cost-effective UP models for optimized deployment requirements.

cnBNG User Plane Architecture

The Cisco IOS XR platforms have a distributed hardware architecture that uses a switch fabric to interconnect a series of chassis slots. Each slot can hold one of several types of line cards (LCs). Each line card in these routers has integrated input-output and forwarding engines. The system can identify and handle the subscriber flow either on the route processor (RP) or on the LC. This architecture thereby provides multiple levels of redundancy and scalability for the subscriber management functionality in cnBNG.

Figure 6: Cloud Native BNG User Plane Architecture





The cnBNG UP architecture is designed to interoperate with cnBNG CP with minimal integration efforts. The main components of cnBNG user plane on the Cisco IOS XR platform are:

- **Subscriber Provisioning Agent (SPA)**—is the common interface to the control plane that is bundled with the existing Cisco IOS XR image. This interface helps to have a minimal configuration requirement to transform from an integrated physical BNG router to a cnBNG user plane. SPA consists of a transport layer at the top that interfaces with the CP, and an API layer at the bottom that isolates the network operating system (NOS) and the CP. This isolation from the NOS helps to make the control plane hardware-agnostic and portable across multicloud environments.

  The functionality of SPA includes:

  - The support for standard PFCP port for a single UP connection.
  - The support for nonstandard ports for both PFCP and GTPv1-U for multiple connections.
  - UP to CP keep alive (KA) to detect any communication channel faults between CP-UP.

- **NOS Adaptation Layer (NAL)**—translates the CP instructions or messages coming to the UP to Cisco IOS XR-defined format. It is the Cisco IOS XR implementation of cnBNG APIs that interfaces with Cisco IOS XR infra components for various functions. These functions include input-output of packets, interface creation and deletion, subscriber feature provisioning, route operations, subscriber interface statistics and notifications. NAL also manages the subscriber flow on the Cisco IOS XR platform and handles the high availability (HA) requirements of Cisco IOS XR infrastructure.

The **cnbng-nal** is the internal process that provisions all the above NAL functionalities. For details on commands that are related to NAL, see the *Configuring Cloud Native BNG User Plane* chapter and the *Verifying Cloud Native BNG User Plane Configurations* chapter.

- **Platform-specific Layer**—is the API adaptation layer that helps to plug-in different types of hardware architectures to the common Cisco IOS XR infrastructure. This layer in turn helps to extend the user plane functionality to other Cisco IOS XR platforms without altering the basic infrastructure.

  Platform-specific layer defines the forward API calls that each underlying platform of the user plane has to implement. The system uses these APIs to provision the following BNG functions:

  - IPoE subscriber traffic classification—for L2-connected subscribers that are based on port, MAC, and VLAN.
  - PPPoE subscriber traffic classification—for L2-connected subscribers that are based on port and PPPoE session-ID.

cnBNG User Plane and Control Plane Reachability

Starting from Release 24.3.1, we support IPv6 transport for the interface between cnBNG and user plane.

For network functionality and interoperability, it is essential to ensure reachability between user plane and control plane using both IPv4 and IPv6. You can set up the user plane to reach control plane either using IPv4 or IPv6 transport, and not both. However, control plane supports multiple user planes configured with IPv4 or IPv6 transport simultaneously.

The protocols used for control plane and user plane communication for exchanging subscriber provisioning messages and protocol packets are:

- PFCP
- GTP-U

Software and Hardware Requirements

The support for cnBNG user plane functionality on Cisco ASR 9000 Series Routers is compatible with the following line card (LC), route switch processors (RSPs), and modular port adapters (MPAs).

Note The Cisco IOS XR Software Release 7.3.1 supports cnBNG UP only on Cisco ASR 9000 High Density 100GE Ethernet line cards. See the table for the list of supported PIDs.

Table 1: Software and Hardware Requirements for cnBNG User Plane

Cisco IOS XR Software Release	LC	RSP	MPA
Cisco IOS XR Software Release 7.3.1	• A9K-24X10GE-1G-SE • A9K-48X10GE-1G-SE • A9K-4X100GE-SE • A9K-MOD200-SE • A9K-MOD200-CM • A9K-MOD400-SE • A9K-MOD400-CM	• A9K-RSP880-SE • A9K-RSP880-LT-SE • A99-RP-SE and A99-RP2-SE (on the Cisco ASR 9912 and the Cisco ASR 9922 chassis) • A99-RSP-SE (on the Cisco ASR 9910 and the Cisco ASR 9906 chassis) • A9K-RSP5-SE	• A9K-MPA-1X100GE • A9K-MPA-2X100GE • A9K-MPA-4X10GE • A9K-MPA-8X10GE • A9K-MPA-20X10GE • A9K-MPA-20X1GE • A9K-MPA-1X40GE • A9K-MPA-2X40GE

Access Types and Subscriber Types

Access Types

The cnBNG user plane on Cisco IOS XR platform supports sub-interface Bundle-Ethernet access type with these encapsulations:

- **Single Dot1q**—which is the IEEE 802.1Q networking standard to support VLANs on an Ethernet network.
- **Double-tagged VLANs**—where two VLAN ID tags (inner tag and outer tag) are inserted into a single data frame. This encapsulation enables users to use their own VLANs inside the VLAN provided by the service provider.
- **Ambiguous VLANs**—that use a range or group of VLAN IDs that enables you to create multiple sessions on a single access-interface.

Subscriber Types

The IP subscriber sessions that connect through a Layer-2 aggregation network are called **L2-connected** sessions. Subscriber sessions where an IPv4 address and an IPv6 address co-exist for the same subscriber are called **dual-stack** subscriber sessions.

The cnBNG UP on Cisco IOS XR platform supports two types of **L2-connected dual-stack** subscriber sessions:

- **IPoE-DHCP dual-stack sessions**: In IP over Ethernet (IPoE) sessions, subscribers run IPv4 or IPv6 on the CPE device and connect to the BNG through an L2 aggregation network. These sessions rely on the DHCP protocol for assigning IP address for the subscriber.

- **PPPoE-DHCPv6 dual-stack PTA sessions**: The PPP over Ethernet (PPPoE) subscriber session is established using the point-to-point protocol (PPP) that runs between the CPE and BNG. These sessions rely on the standard PPP negotiations for subscriber authentication and IP address assignment.

  In a PPP Termination and Aggregation (PTA) session, the PPP encapsulation terminates on BNG. After that the BNG routes the traffic to the service provider using IP routing.

Subscriber Features

Table 2: Feature History Table

Feature Name	Release Information	Feature Description
Increased Granularity for Cloud Native BNG Traffic Management with Hierarchical QoS (H-QOS)	Release 7.4.2	This feature allows you to specify QoS behavior at multiple policy levels for Internet Protocol over Ethernet (IPoE), Point-to-Point Protocol over Ethernet (PPPoE), PPP Termination and Aggregation (PTA), and LNS (L2TP Network Server) sessions and provides a high degree of granularity in traffic management. Use the first level of the traffic policy, the parent traffic policy, to control the traffic at the main interface or sub-interface level. Use the second level, the child traffic policy, for additional control over a specific traffic stream or class.
Multiple Framed IPv4 and IPv6 Routes for Customer PremisesEquipment (CPE)	Release 7.4.2	You can configure multiple framed routes for IPv4 and IPv6 traffic across CPE. This functionality allows you to route multiple customer networks through a single customer broadband connection, thus enabling the LAN network subscriber to use a different subnet from WAN.

Feature Name	Release Information	Feature Description
Cloud Native BNG feature extension to 5th Generation Line Card	Release 7.4.2	The A99-32X100GE-X-SE, A9K-20HG-FLEX-SE , and A9K-8HG-FLEX-SE line cards now support the following Cloud Native BNG functionalities: • IPoE subscriber sessions that run both IPv4, IPv6 on the CPE device. • PPP over Ethernet PPP Termination and Aggregation (PPPoE PTA) sessions • DHCPv6 support for PPPoE sessions • Cloud Native BNG over Bundle Ether interface • Quality of Service (QoS) • Policy-based Routing (PBR) • Access Control List (ACL) • ICMP unreachable • Lawful Intercept (LI) This enhancement enables BNG features to leverage the higher throughput of the 5th generation of line cards.

This section lists the set of subscriber features that cnBNG user plane on the Cisco IOS XR platform supports.

- **IPv4 or IPv6**:
  - **Maximum Transmission Unit (MTU)**—that defines the maximum size of each packet that you can transmit during the subscriber session.
  - **Unicast Reverse Path Forwarding (URPF)**—that ensures that the system does not accept any traffic on the subscriber interface from malformed or forged IP source addresses.
  - **Internet Control Message Protocol (ICMP)**—a supporting protocol that networking devices use to send error messages and operational information to the originator of transmission.
- **Access Control List (ACL)**—that performs packet filtering to control the traffic flow into and out of network interfaces. It helps to define the access rights such as, filtering the content, blocking access to various resources and so on, for a subscriber .

  Supported ACL types are:
  - Input ACL (IPv4 or IPv6)

- Output ACL (IPv4 or IPv6)

- **QoS**:
  - **Policing (input and output)**—that allows you to control the maximum rate of traffic sent or received on an interface. It also allows to partition a network into multiple priority levels or class of service (CoS).
  - **Shaping (output)**—that allows you to control the traffic flow that exits an interface to match its transmission to the speed of the remote target interface. It also ensures that the traffic conforms to policies contracted for it.
  - **Policy Merging**—that merges multiple QoS policies on a single subscriber. The UP supports a maximum of 6 policy-maps and 10 class-maps, including the default ones.

- **Hierarchical QoS (H-QoS)**—that allows you to specify QoS behavior at multiple policy levels, which provides a high degree of granularity in traffic management. cnBNG supports the following two-level hierarchical policy for deploying QoS:
  - Parent policy:
  - Child policy

  H-QoS is applied on the router interface using nested traffic policies. The first level of traffic policy, the parent traffic policy, is used for controlling the traffic at the main interface or sub-interface level. The second level of traffic policy, the child traffic policy, is used for additional control over a specific traffic stream or class. The child traffic policy, is a previously defined traffic policy, that is referenced within the parent traffic policy. Two-level H-QoS is supported on both ingress and egress directions on all line cards and on physical or bundle main interfaces and sub-interfaces.

  To know more about H-QOS, refer the *Configuring Hierarchical Modular QoS* chapter in the *Modular QoS Configuration Guide for Cisco ASR 9000 Series Routers*

- **HTTP Redirect using PBR** (for input policy)—that redirects subscriber traffic to a destination other than to its original destination. Policy-based Routing (PBR) makes packet forwarding decisions based on the policy configurations, instead of routing protocols.
- **Accounting:** cnBNG UP supports periodic accounting for these accounting types:
  - **Session Accounting**—which is the statistics of a subscriber session.
  - **Service Accounting:**—which is the statistics for each service (collection of features) that is enabled for a subscriber.

Note
- You cannot enable service accounting without session accounting.
- You cannot have different periodicity for session and service accounting.

- **Lawful Intercept** (for mediation device in default or non-default VRF)—that allows Law Enforcement Agencies (LEA) to conduct electronics surveillance as authorized by judicial or administrative order.
- **Multiple Framed Route**—allows a large number of customer networks to reach through framed routes through a single broadband connection. Framed Route is supported on both IPoE and PPPoE sessions.

There’s no limit enforced to the number of framed routes per session. You don't have to configure or enable Framed Route through command line interface as it is downloaded from RADIUS.

Read more about these features in the *Cisco ASR 9000 Series Aggregation Services Router Broadband Network Gateway Configuration Guide*.

Supported Parameter Limit for Subscriber Features

The cnBNG user plane on Cisco IOS XR platform supports a maximum of:

- 32 IP subnet pools
- 32 secondary IP addresses
- Eight QoS services
- Eight class-maps
- Six actions for multi-action change-of-authorization (MA-CoA)

  (MA-CoA is a feature which enables the service providers to activate and deactivate multiple subscriber services using a single CoA request).

High Availability

High Availability (HA) enables network-wide protection by providing fast recovery from faults that may occur in any part of the network. The cnBNG user plane does not delete the subscriber state, summary subnet route state, subscriber route state, and so on, in a stable system except in a few scenarios. These scenarios can be either explicit execution of CLI commands to clear the session, process restart of peer process, mark and sweep procedure (an internal clean-up process which detects and reclaims the memory that is used by unused objects) of *cnbng-nal* process, route processor fail over (RPFO), or deletion of parent interface.

This section describes the expected behavior if a high availability event such as a router reload or RPFO occurs on the cnBNG user plane:

- NAL restores the last stable (check-pointed) session state with best effort after the HA event.
- To ensure data and session integrity between NAL and peer processes, the system triggers a mark and sweep procedure during *cnbng-nal* process restart. During this process, the NAL might not be able to restore the sessions due to unforeseen issues from the feature or from the IOS XR infra components. In that case, the system deletes those sessions and sends a notification to the CP.
- The *cnbng-nal* process restart does not initiate automatic reconciliation procedure between the CP and the UP. The CP triggers this explicitly using a CLI configuration.
- The Cisco IOS XR platform has active and standby hardware level support (active RSP and standby RSP) on logical interface subscriber. The data sync between these nodes is not real time. The *cnbng-nal* process periodically syncs for various internal data on a best-effort basis. There can be a few cases where session data is out of sync between route processors which leads to session recreate failure after RFPO. These cases maybe for recently created sessions or inflight sessions. The system deletes those sessions at UP and sends a notification to the CP.
- The CP acts on these notification events to make sure that the subscriber state is in sync. If not, it leads to out of sync sessions between the UP and the CP in such scenarios.

- During process restart or RPFO, mark and sweep procedure might lead to subscriber session deletion on UP.
- The UP might not push the final statistics if a process restart or RPFO happens while a subscriber or service deletion is in progress. In that case, the CP considers the last collected statistics PCRF or back-end statistics as the final statistics.

Usage Guidelines

These guidelines apply to using the cnBNG user plane functionality on the Cisco IOS XR platform:

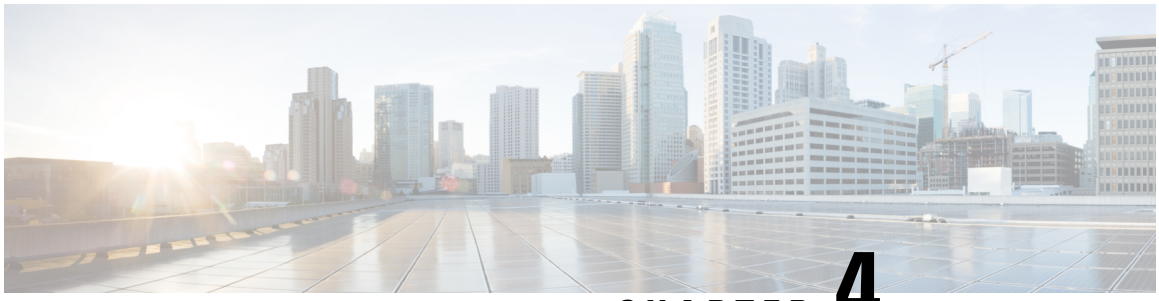
- You must not perform these actions on the fly while active subscriber sessions are present on the router:
  - Removal of configurations
  - Enabling or disabling service accounting
  - Deletion or modification of parent interface properties (such as IPv4 or IPv6 address, MTU, DHCPv4 initiator, PPPoE, DHCPv6 initiator, enable L2TP and LNS, and so on)
  - Deactivation of cnBNG package
  - Deletion or modification of VRF and loopback
  - Modification of service profile, and IPv4 or IPv6 address
- PPP keep alive (KA)—the user plane generates the PPP KA messages to the CPE to make packet transport more efficient between the CP and the UP. You must ensure that the duration of PPP keep alive is large enough (in tens of minutes) to have better CPU performance in scenarios with large subscriber scale.
- If an update request having service deactivation fails, the UP reactivates the service as part of rollback and starts the statistics afresh from zero.
- The CP-UP communication loss might cause the CP and UP to be in out of sync. There is no automated recovery mechanism for such scenarios.

Restrictions

The cnBNG user plane functionality on the Cisco IOS XR platform does not support these functionalities:

- Standalone PPP use case with cnBNG enabled
- Multiple loopbacks under a single VRF
- Per pool or VRF tag support for IP pool subnet routes installed with a specific tag for the entire UP
- Back-to-back RPFO or switchover without graceful shutdown
- LC-based subscribers
- Subscriber redundancy group (SRG) for Bundle-Ethernet
- Enabling service accounting without session accounting

- Different periodicity for session and service accounting



CHAPTER 4

Installing Cloud Native BNG User Plane Packages

This chapter describes the procedure for installing cloud native BNG user plane packages on Cisco IOS XR platform.

Installing and Activating the cnBNG Package on the User Plane

Before you begin:

You must follow these guidelines before installing cnBNG package on the user plane:

- The cnBNG user plane functionality requires two packages to be installed on the router—the BNG support package (**asr9k-bng-supp-x64-*.rpm**) and the cnBNG package **(asr9k-cnbng-x64-*.rpm**).
- You can install cnBNG as an optional package on the router. The standard Cisco Golden ISO (GISO) image does not contain the cnBNG package.
- The physical BNG package (**asr9k-bng-x64*.rpm**) and the cnBNG package (**asr9k-cnbng-x64*.rpm**) are mutually exclusive. You cannot install both the packages on the router. The install operation fails if tried.
- You must uninstall and remove the physical BNG package and reboot the router prior to installing the cnBNG package on a router which is already being used as a physical BNG.
- You can either activate the BNG support package and the cnBNG package together as a single step or activate the BNG support package first and then activate the cnBNG package.
- The system does not support standalone PPP use case with cnBNG enabled. You must remove any PPP configuration before activating cnBNG on the router.

Installing and Activating the cnBNG Package on the User Plane

- **Step 1**: Install both the BNG support package and the cnBNG package from the RPM location to the router

  Use the **install add source** command.

```
Router#install add source tftp://209.165.200.225/test-path/
asr9k-bng-supp-x64-1.0.0.0-r73105I.x86_64.rpm asr9k-cnbng-x64-1.0.0.0-r73105I.x86_64.rpm
```

This step adds the BNG support package (**asr9k-bng-supp-x64-1.0.0.0-r73105I.x86_64.rpm**) and the cnBNG package (**asr9k-cnbng-x64-1.0.0.0-r73105I.x86_64.rpm**) from the source location of the RPMs (**tftp://209.165.200.225/test-path/**) to the router.

- **Step 2:** Activate the packages

  Use the **install activate** *activate-id* command.

  Where, *activate-id* is the ID that you see on the router console once the **install add** operation in the previous step is completed.

```
Router#install activate 1
```

  This step activates both the BNG support package and the cnBNG package which were installed as part of step 1.

- **Step 3:** Verify the activated packages.

  Use the **show install active** command.

```
Router#show install active
Sun Apr 19 09:49:34.041 UTC
Node 0/RSP0/CPU0 [RP]
  Boot Partition: xr_lv0
  Active Packages: 5
        asr9k-xr-7.3.1.05I version=7.3.1.05I [Boot image]
        asr9k-bng-supp-x64-1.0.0.0-r73105I
        asr9k-cnbng-x64-1.0.0.0-r73105I

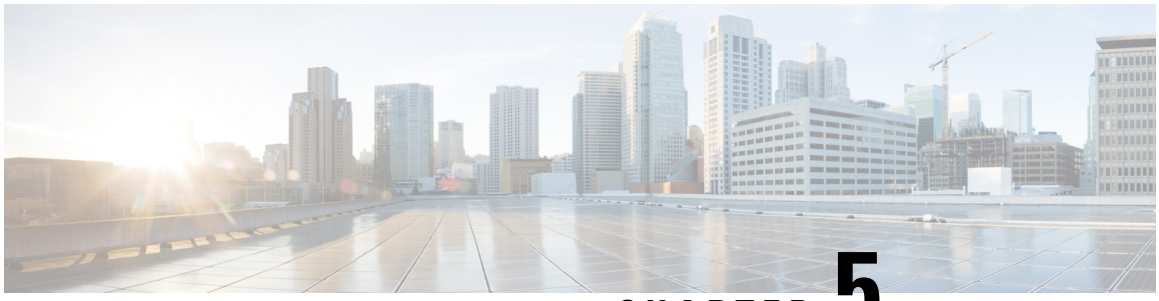
Node 0/0/CPU0 [LC]
  Boot Partition: xr_lv0
  Active Packages: 5
        asr9k-xr-7.3.1.05I version=7.3.1.05I [Boot image]
        asr9k-bng-supp-x64-1.0.0.0-r73105I
        asr9k-cnbng-x64-1.0.0.0-r73105I

Node 0/1/CPU0 [LC]
  Boot Partition: xr_lv0
  Active Packages: 5
        asr9k-xr-7.3.1.05I version=7.3.1.05I [Boot image]
        asr9k-bng-supp-x64-1.0.0.0-r73105I
        asr9k-cnbng-x64-1.0.0.0-r73105I

Node 0/3/CPU0 [LC]
  Boot Partition: xr_lv0
  Active Packages: 5
        asr9k-xr-7.3.1.05I version=7.3.1.05I [Boot image]
        asr9k-bng-supp-x64-1.0.0.0-r73105I
        asr9k-cnbng-x64-1.0.0.0-r73105I
```

  The *Active Packages* parameter in the show command output lists the BNG support package and the cnBNG package. This shows successful activation of the packages.

This step completes the installation and activation of cnBNG package on the user plane.



CHAPTER 5

Configuring Cloud Native BNG User Plane and Key Features

This chapter describes the configuration procedures to achieve the cnBNG user plane functionality on Cisco ASR 9000 Series Routers.

For details on cnBNG user plane commands, see the *Cloud Native BNG Command Reference for Cisco ASR 9000 Series Routers*.

Configure cnBNG User Plane

Before you begin:

You must follow these guidelines for configuring cnBNG user plane:

- You must perform a complete reimage followed by a reboot of the router if you are switching between physical BNG to cnBNG, or the other way around.
- Ensure that the cnBNG package is installed and activated on the user plane. See the *Installing Cloud Native BNG User Plane Packages* chapter for detailed procedure.
- The system does not support the removal of configurations while active sessions are present. You must delete all active sessions and dissociate the CP-UP connection prior to any configuration change or commit replace procedure.

Configuration Procedure

You must perform the following tasks for the UP to spawn the NAL process, to establish connection with the CP, and to provision the subscriber requests.

Configure Basic User Plane Settings

The basic user plane configuration for cnBNG involves these high-level tasks:

- Configuring the server endpoints of CP to which UP can send PFCP or GTP-U messages to enable cnBNG on the router.
- Configuring a loopback interface for each VRF.
- Configuring a route tag for subscriber summary routes.
- Configuring the access-interface to enable IPoE and PPPoE subscribers.

The cnBNG endpoint configurations on the UP are delivered to the cnBNG SPA component for initiating connection with the CP.

Configuration Procedure

This section describes the steps for the basic user plane configuration, which include certain mandatory and optional configurations.

Mandatory Configurations:

- Specifying a unique name for the UP-server instance.
- Specifying the details of the UP server (such as IP address, GTP port, and PFCP port) to which the CP can send PFCP or GTP-U messages.
- Specifying the details of CP server to which the UP can send PFCP or GTP-U messages.
- Specifying the retry count for CP-UP association.
- Enabling secondary address programming.
- Specifying a name for the auto-loopback VRF.
- Configuring a loopback interface to associate with the above VRF.
- Specifying a primary address for the loopback interface.

Optional Configuration:

- Configuring a route summary tag for the routes to add in the routing table

Configuration Example

Configuration example with IPv4 transport.

```
Router#configure
Router(config)#cnbng-nal location 0/RSP0/CPU0
Router(config-cnbng-nal-local)#hostidentifier asr9k-1
Router(config-cnbng-nal-local)#cp-server primary ipv4 198.51.100.1
Router(config-cnbng-nal-local)#up-server ipv4 192.0.2.1 gtp-port 15002 pfcp-port 15003 vrf
 default
Router(config-cnbng-nal-local)#secondary-address-update-enable
Router(config-cnbng-nal-local)#cp-association retry-count 10
Router(config—cnbng-nal-local)#auto-loopback vrf test
Router(config—cnbng-nal-local-auto-loopback-vrf)#interface Loopback2
Router(config—cnbng-nal-local-auto-loopback-vrf-int)#primary-address 127.0.0.1
Router(config—cnbng-nal-local-auto-loopback-vrf-int)#exit
Router(config—cnbng-nal-local-auto-loopback-vrf)#exit
/* Auto-loopback configuration for default VRF */
Router(config—cnbng-nal-local)#auto-loopback vrf default
```

```
Router(config—cnbng-nal-local-auto-loopback-vrf)#interface Loopback1
Router(config—cnbng-nal-local-auto-loopback-vrf-int)#primary-address 10.0.0.1
Router(config—cnbng-nal-local-auto-loopback-vrf-int)#exit
Router(config—cnbng-nal-local-auto-loopback-vrf)#exit
Router(config-cnbng-nal-local)#route-summary tag 4
Router(config-cnbng-nal-local)#commit
```

Running Configuration

```
Router#show running-config cnbng-nal location 0/RSP0/CPU0
cnbng-nal location 0/RSP0/CPU0
 hostidentifier asr9k-1
 up-server ipv4 192.0.2.1 vrf default
  gtp-port 15002
  pfcp-port 15003
 cp-server primary ipv4 198.51.100.1
 secondary-address-update-enable
cp-association retry-count 10
auto-loopback vrf test
 interface Loopback2
  primary-address 127.0.0.1
 !
!
auto-loopback vrf default
 interface Loopback1
  primary-address 10.0.0.1
 !
!
route-summary tag 4
!
```

Configure Access-Interface

This section describes how to configure the access-interface and to enable PPPoE on the cnBNG user plane.

Configuration Example

```
Router#configure
Router(config)#interface Bundle-Ether1.1
Router(config-subif)#ipv4 point-to-point
Router(config-subif)#ipv4 unnumbered Loopback1
Router(config-subif)#ipv6 enable
Router(config-subif)#encapsulation dot1q 1
Router(config-subif)#ipsubscriber
Router(config-cnbng-nal-ipsub)#ipv4 l2-connected
Router(config-cnbng-nal-ipsub-l2conn)#initiator dhcp
Router(config-cnbng-nal-ipsub-l2conn)#exit
Router(config-cnbng-nal-ipsub)#ipv6 l2-connected
Router(config-cnbng-nal-ipsub-ipv6-l2conn)#initiator dhcp
Router(config-cnbng-nal-ipsub-ipv6-l2conn)#exit
Router(config-cnbng-nal-ipsub)#exit

/* Enable PPPoE */
Router(config-subif)#pppoe enable
Router(config-subif)#commit
```

Running Configuration

```
Router#show running-config interface be1.1
interface Bundle-Ether1.1
 ipv4 point-to-point
 ipv4 unnumbered Loopback1
 ipv6 enable
 encapsulation dot1q 1
 ipsubscriber
  ipv4 l2-connected
   initiator dhcp
  !
  ipv6 l2-connected
   initiator dhcp
  !
 !
 pppoe enable
!
```

Configure Loopback Interface

This section describes how to configure the loopback interface for cnBNG user plane.

Note You must not configure any IP address under loopback interface.

Configuration Example

```
Router#configure
Router(config)#interface loopback 2
Router(config-if)#ipv6 enable
Router(config-if)#commit
```

Running Configuration

```
Router#show running-config interface loopback 2
interface Loopback2
 ipv6 enable
!
```

Configure DHCP

This section describes the steps to configure DHCP for cnBNG BNG user plane.

The basic DHCP configurations include these steps:

- Creating a cnBNG profile
- Assigning the cnBNG profile to access-interfaces

Configuration Example

```
Router(config)#dhcp ipv4
/* Create a cnBNG profile */
Router(config-dhcpv4)#profile cnbng_1 cnbng
Router(config-dhcpv4-cnbng-profile)#exit
/* Assign the cnBNG profile to access-interfaces */
Router(config-dhcpv4)#interface bundle-Ether 1.1 cnbng profile cnbng_1
Router(config-dhcpv4)#interface bundle-Ether 2.1 cnbng profile cnbng_1
Router(config-dhcpv4)#commit
```

Similarly, you can configure the DHCP IPv6 profiles.

Running Configuration

```
Router#show run dhcp ipv4
Wed Oct 14 16:48:56.814 UTC
dhcp ipv4
 profile cnbng_1 cnbng
 !
 interface Bundle-Ether1.1 cnbng profile cnbng_1
 interface Bundle-Ether2.1 cnbng profile cnbng_1
!


Router#show run dhcp ipv6
Wed Oct 14 16:49:19.095 UTC
dhcp ipv6
 profile cnbng_1 cnbng
 !
 interface Bundle-Ether1.1 cnbng profile cnbng_1
 interface Bundle-Ether2.1 cnbng profile cnbng_1
!
```

Configure Subscriber Gateway Address and Subnet Route

Table 3: Feature History Table

Feature Name	Release Information	Feature Description
Disable Notifications for Dynamic Programming of Subscriber Gateway Address	Release 7.4.2	This feature allows you to disable the notifications exchanged internally between software components when the user plane (UP) of a cloud-native BNG (cnBNG) network programs the gateway address for its subscriber. It prevents excessive notifications when many active subscribers are on the UP, thus reducing the overhead on UP resources. The feature introduces the following command: • disable-secondary-address-notification

In cnBNG, the IP address management is more dynamic. Hence, the loopback interface for IPoE or PPPoE subscribers isn't provisioned in the user profile of the subscriber with static configuration. cnBNG user plane selects the loopback based on the subnet allocated to a loopback dynamically at cnBNG user plane.

Note For every VRF, one loopback must be present on the UP.

Consider this example,

```
On RSP0:
Tue Jul 28 05:55:13.015 UTC
cnbng-nal location 0/RSP0/CPU0
hostidentifier asr9k-1
up-server ipv4 192.0.2.1 vrf default
cp-server primary ipv4 198.51.100.1
auto-loopback vrf default
  interface Loopback1
   primary-address 10.0.0.1
  !
!
On RSP1:
Tue Jul 28 05:56:13.015 UTC
cnbng-nal location 0/RSP1/CPU0
hostidentifier asr9k-1
up-server ipv4 192.0.2.1 vrf default
cp-server primary ipv4 198.51.100.1
auto-loopback vrf default
  interface Loopback1
   primary-address 10.0.0.1
  !
!
```

In this example, the CP assigns 10.11.12.0/24 as subnet, and 10.11.12.1/32 as gateway address to subscribers under the default VRF. This gateway address serves as the DHCPv4 server address for DHCPv4 OFFER or ACK messages. The *cnbng-nal* process uses Operations Center (OC) to configure this gateway address as secondary IP address on the loopback and route provision APIs to program the entry in the L3 routing table.

Note The system supports a maximum of 32 secondary IP addresses under an interface.

```
Router#show ipv4 interface loopback 1
Tue Jul 28 05:29:58.741 UTC
Loopback1 is Up, ipv4 protocol is Up
  Vrf is default (vrfid 0x60000000)
  Internet address is 10.0.0.1/32
  Secondary address 10.11.12.1/32


Router#show route vrf all ipv4 subscriber
A    10.11.12.0/24 [1/0] via 0.0.0.0, 00:10:29
```

Note The dynamic programming of the subnet (secondary gateway) under the loopback causes a major churn on the UP if large scale of active subscribers is present on the node. Hence, the secondary address programming is disabled, by default.

Enable Secondary Address Programming

It's mandatory to enable the secondary address programming on cnBNG user plane. To enable that, use the **secondary-address-update enable** command under the cnbng-nal configuration mode.

Configuration Example

```
Router#configure
Router(config)#cnbng-nal location 0/RSP0/CPU0
Router(config-cnbng-nal)#secondary-address-update enable
Router(config-cnbng-nal)#commit
```

Running Configuration

```
Router#show running-config cnbng-nal location 0/RSP0/CPU0
cnbng-nal location 0/RSP0/CPU0
 secondary-address-update enable
!
```

Note From Release 7.4.2 onwards, you can disable internal notifications on the UP while it programs the secondary address on the loopback interface by configuring the command **disable-secondary-address-notification**.

Disable Notifications for Dynamic Programming of Subscriber Gateway Address

In a cnBNG network, the CP assigns the gateway address for each subscriber. The UP dynamically programs gateway address assigned to each subscriber as a secondary IP address on its loopback interface. During this configuration, UP internally exchanges notification messages between various software components. The more the number of active subscribers on the UP, the more the notifications. To preserve valuable time and resources of the UP, you can disable notifications using the command **disable-secondary-address-notification** in the **cnbng-nal-local** config mode.

Configuration Example

```
Router#configure
Router(config)#cnbng-nal location 0/RSP0/CPU0
Router(config-cnbng-nal-local)#disable-secondary-address-notification
Router(config-cnbng-nal-local)#commit
```

Running Configuration

The following running configuration on cnBNG UP includes basic UP configuration as well:

```
Router#show running-config cnbng-nal location 0/RSP0/CPU0
cnbng-nal location 0/1/CPU0
 hostidentifier RTR1
 auto-loopback vrf test
  interface Loopback1
   primary-address 10.1.1.1
  !
 !
 auto-loopback vrf default
  interface Loopback0
   primary-address 10.30.30.1
  !

 !

 up-server ipv4 10.11.11.1 gtp-port 15002 pfcp-port 15003 vrf default
 cp-server primary ipv4 10.11.11.2
 enable-test-server
 disconnect-history file-logging-enable
 secondary-address-update enable
 disable-secondary-address-notification
 route-summary tag 111
 cp-association retry-count 5
!
```

Configure Route Summary

This section describes the steps to configure route summary for the cnBNG user plane.

The NAL handles the following routes:

- Individual subscriber routes
- Summary routes for subscriber pool subnet

The subscriber routes are part of the subscriber provisioning message, which includes:

- WAN IP address (/32 or /128 subnet)
- LAN IP (prefix delegation)

The summary routes are for the subscriber pool subnet which are exported to the core network to download traffic towards the subscriber. On physical BNG, the subscriber pool subnets were configured as static routes and redistributed through BGP or IGP. With cnBNG and auto-loopback selection, these subnets for the subscribers are added dynamically to the loopback. Every time a new subscriber pool subnet is added to the loopback, the same is added to the RIB with the tag that is provided by the CP. If tag is '0', the NAL uses the tag configured under the cnbng-nal. Routes with this tag can be exported to the core using the Routing Protocol for Low-Power and Lossy Networks (RPLs).

To configure route summary, use the **route-summary** command under the cnbng-nal configuration mode.

Configuration Example

```
Router#configure
Router(config)#cnbng-nal location 0/RSP0/CPU0
Router(config-cnbng-nal)#route-summary tag 10
Router(config-cnbng-nal)#commit
```

Running Configuration

```
Router#show running-config cnbng-nal location 0/RSP0/CPU0
cnbng-nal location 0/RSP0/CPU0
 route-summary tag 10
!
```

After the first subnet is installed on NAL, the following routes are added to the system:

```
A 10.11.12.0/24 [1/0] via 0.0.0.0, 0d01h
```

Export Routes to Core Network

This section describes how to export routes to core network as part of enabling cnBNG user plane functionality.

Configuration Example

```
Router#configure
Router(config)#route-policy test-policy-cnbng
Router(config-rpl)#if tag eq 10 then
Router(config-rpl-if)#set community (123:100)
Router(config-rpl-if)#done
Router(config-rpl-if)#endif
Router(config-rpl)#end-policy
Router(config)#commit

Router(config)#router ospf 10
Router(config-ospf)#vrf test-vrf-cnbng
Router(config-ospf-vrf)#redistribute subscriber route-policy test-policy-cnbng
Router(config-ospf-vrf)#commit
```

Running Configuration

```
Router#show running-config route-policy test-policy-cnbng
route-policy test-policy-cnbng

     if tag eq 10  then

       set community (123:100)

       done

     endif

   end-policy
   !

Router#show running-config router ospf
router ospf 10
 vrf test-vrf-cnbng
  redistribute subscriber route-policy test-policy-cnbng
  !
```

Configure ARP Scale Mode

This section describes the steps to configure ARP scale mode for the cloud-native BNG user plane.

To disable interface entry creation by ARP for each subscriber interface on the data plane (line cards), you must enable ARP scale mode for the subscriber using the **arp scale-mode-enable** command in subscriber configuration mode.

Configuration Example

```
Router#configure
Router(config)#subscriber
Router(config-subscriber)#arp scale-mode-enable
Router(config-subscriber)#commit
```

Running Configuration

```
Router#show running-config subscriber
Sat Aug 22 06:36:21.422 UTC
subscriber
arp scale-mode-enable
!
```

Configure Cloud Native BNG over Pseudowire Headend

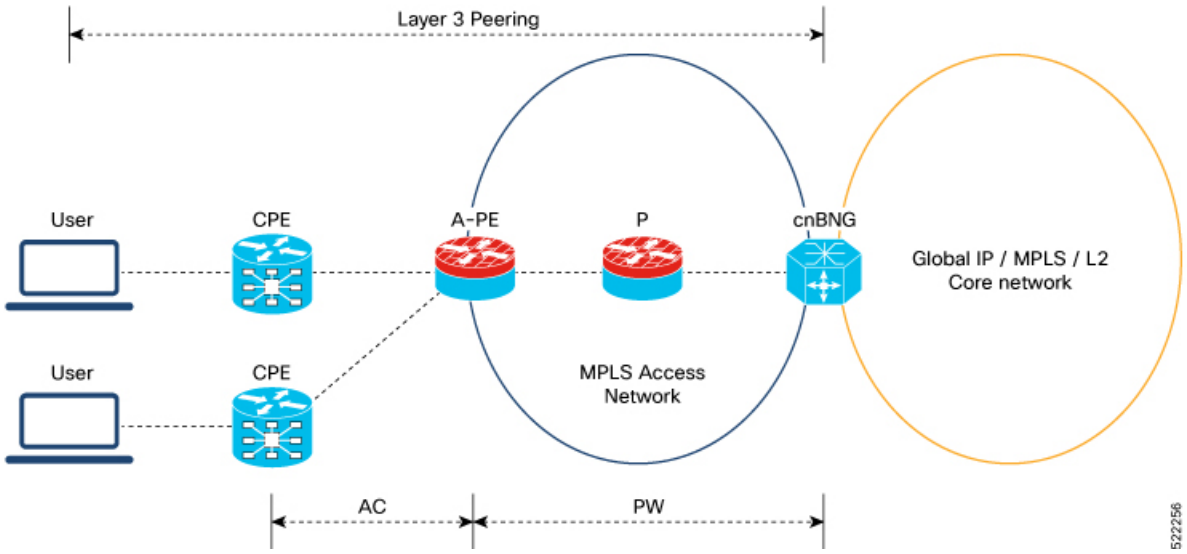
Table 4: Feature History Table

Feature Name	Release Information	Feature Description
Establishing Cloud Native BNG Sessions over Pseudowire Headend (PWHE)	Release 7.4.2	This feature establishes Cloud Native BNG subscriber sessions on PWHE interfaces. PWHE enables an easy and scalable mechanism for tunneling cnBNG traffic into a common IP, MPLS, or L2 network.

Cloud Native BNG provides subscriber support over Pseudowire Headend (PWHE). PWHE provides L3 connectivity to customer edge nodes through a pseudowire connection. PWHE terminates the L2VPN circuits that exist between the access-provide edge (A-PE) nodes, to a virtual interface, and performs routing on the native IP packet. Each virtual interface can use one or more physical interfaces towards the access cloud to reach customer Router through the A-PE nodes.

This figure shows a sample topology for Cloud Native BNG over Pseudowire Headend:

Figure 7: Sample Topology for Cloud Native BNG over Pseudowire Headend:



Restrictions

You can not configure eight ECMP links on the same PE device.

Configuration Example

This section provides the sample configurations for BNG over Pseudowire Headend:

The following is the sample configuration to allow IPOE or PPPOE subsciber to bring up from the PWHE access interface on the cnBNG:

```
Router#configure
```

```
Router(config)#interface PW-Ether100.102
Router(config-subif)#ipv4 unnumbered Loopback100
Router(config-subif)#ipv6 enable
Router(config-subif)#load-interval 30
Router(config-subif)#ipsubscriber
Router(config-cnbng-nal-ipsub)#ipv4 l2-connected
Router(config-cnbng-nal-ipsub-l2conn)#initiator dhcp
Router(config-cnbng-nal-ipsub-l2conn)#exit
Router(config-cnbng-nal-ipsub)#ipv6 l2-connected
Router(config-cnbng-nal-ipsub-ipv6-l2conn)#initiator dhcp
Router(config-cnbng-nal-ipsub-ipv6-l2conn)#exit
Router(config-cnbng-nal-ipsub)#exit
Router(config-subif)#pppoe enable
Router(config-subif)#encapsulation ambiguous dot1q any second-dot1q 102
Router(config-subif)#commit
```

This example shows the configuration of DHCPv4 on PWHE interfaces:

```
Router#configure
Router(config)#dhcp ipv4
Router(config-dhcpv4)#profile cn4 cnbng
Router(config-dhcpv4-cnbng-profile)#exit
Router(config-dhcpv4)#interface PW-Ether100.102 cnbng profile cn4
Router(config-dhcpv4)#interface PW-Ether100.103 cnbng profile cn4
Router(config-dhcpv4)#interface PW-Ether100.104 cnbng profile cn4
Router(config-dhcpv4)#commit
```

This example shows the configuration of DHCPv6 on PWHE interface:

```
Router#configure
Router(config)#dhcp ipv6
Router(config-dhcpv6)#profile cn4 cnbng
Router(config-dhcpv6-cnbng-profile)#exit
Router(config-dhcpv6)#interface PW-Ether100.102 cnbng profile cn6
Router(config-dhcpv6)#interface PW-Ether100.103 cnbng profile cn6
Router(config-dhcpv6)#commit
```

Running Configuration

The following example displays the running configuration of pw-ether interface.

```
Router#show running-config interface PW-Ether 100.102
Thu Feb  3 11:33:58.450 IST
interface PW-Ether100.102
 ipv4 unnumbered Loopback100
 ipv6 enable
 load-interval 30
 ipsubscriber
  ipv4 l2-connected
   initiator dhcp
  !
  ipv6 l2-connected
   initiator dhcp
  !
 !
 pppoe enable
 encapsulation ambiguous dot1q any second-dot1q 102
!
```

Configure DHCPv4 on PWHE interface:

```
Router#show run dhcp ipv4
Thu Feb  3 11:55:01.903 IST
dhcp ipv4
 profile cn4 cnbng
 !
 interface PW-Ether100.102 cnbng profile cn4
 interface PW-Ether100.103 cnbng profile cn4
 interface PW-Ether100.104 cnbng profile cn4
!
```

Configure DHCPv6 on PWHE interface:

```
Router#show run dhcp ipv6
Thu Feb  3 11:55:07.906 IST
dhcp ipv6
 profile cn6 cnbng
 !
 interface PW-Ether100.102 cnbng profile cn6
 interface PW-Ether100.103 cnbng profile cn6
!
```

Verify cnBNG User Plane Configuration

This section describes the show commands to be executed on the router to verify cloud native BNG user plane configuration.

For details on cnBNG commands, see the *Cloud Native BNG Command Reference for Cisco ASR 9000 Series Routers*.

Verify cnBNG NAL Process Information

You can use the following commands to verify the NAL process information on cnBNG user plane.

-
```
Router#show cnbng-nal process-info location 0/RSP0/CPU0
Mon Aug  3 00:12:42.080 UTC

Location: 0/RSP0/CPU0

 HA Pre_Init Role          : PRIMARY
 HA Role                   : PRIMARY
 Restart-flag              : FALSE
 card_type                 : 0
 Node-Id                   : 0
 Disc-Hist File-logging    : FALSE
 Test-server config-enabled: FALSE

 Proc-flags     : 8000FFBF

    OT Connection Status: UP
    IM Connection Status: UP
    IPv4 RIB Connection Status: UP
    IPv6 RIB Connection Status: UP
    SUBDB Connection Status: UP
```

-
```
Router#show cnbng-nal process-readiness
Mon Aug  3 00:12:00.778 UTC

Location: 0/RSP1/CPU0

NAL resync pending flags:
        Service Resync Pending
        Interface Resync Pending
        IPv4 Route Resync Pending
        IPv6 Route Resync Pending

SIR status: not ready

Location: 0/RSP0/CPU0
NAL resync pending flags:
        NONE

SIR status: ready
```

-
```
Router#show processes cnbng_nal
Fri Sep 11 09:22:45.139 UTC
                  Job Id: 456
                     PID: 1543

Router#show processes memory 1543
Fri Sep 11 09:24:12.398 UTC
JID      Text(KB)   Data(KB)  Stack(KB) Dynamic(KB) Process
------ ---------- ---------- ---------- ----------- ------------------------------
456           992    1700604        200       19999 cnbng_nal
```

Verify Control Plane Connection Status

You can use the following command to verify the connection status of cnBNG control plane.

-
```
Router#show cnbng-nal cp connection status
Fri Feb 19 11:27:31.178 UTC

Location: 0/RSP0/CPU0


User-Plane configurations:
--------------------------
IP             : 10.105.227.96
 GTP Port       : 2152
PFCP Port      : 8805
VRF            : default


Control-Plane configurations:
-----------------------------
PRIMARY IP     : 10.84.102.235
 GTP Port       : 2152
PFCP Port      : 8805

 Association retry count: 10

Connection Status: Up
```

```
Connection Status time stamp: Thu Feb 11 12:46:19 2021

Connection Prev Status : Down
Connection Prev Status time stamp: Thu Feb 11 12:44:55 2021

Association status: Active
Association status time stamp: Thu Feb 11 12:46:18 2021
```

Verify Subscriber Information

You can use the following commands to verify subscriber information on the cnBNG user plane.

-

```
Router#show cnbng-nal subscriber access-interface bundle-Ether 1.1
Mon Aug  3 00:04:42.558 UTC
=====================
Location: 0/RSP0/CPU0
=====================

               Type            PPPoE           IPoE
               ====            =====           ====

Session Counts by State:
        initializing           0               0
          connecting           0               0
           connected           0               0
           activated           0               8000
                idle           0               0
       disconnecting           0               0
              Total:           0               8000


Session Counts by Address-Family:
               none            0               0
               ipv4            0               0
               ipv6            0               8000
               dual            0               0
              Total:           0               8000


=====================
Location: 0/RSP1/CPU0
=====================

               Type            PPPoE           IPoE
               ====            =====           ====

Session Counts by State:
        initializing           0               0
          connecting           0               0
           connected           0               0
           activated           0               8000
                idle           0               0
       disconnecting           0               0
              Total:           0               8000


Session Counts by Address-Family:
               none            0               0
               ipv4            0               0
               ipv6            0               8000
```

```
                dual            0               0
               Total:           0               8000
```

-

```
Router#show cnbng-nal subscriber all
Fri Sep 11 06:07:52.343 UTC
   Codes: CN - Connecting, CD - Connected, AC - Activated,

        ID - Idle, DN - Disconnecting, IN - Initializing



CPID(hex)Interface            State Mac Address    Subscriber IP Addr / Prefix (Vrf)
Ifhandle
-------------------------------------------------------------------------------------------

1005ca0  BE2.500.ip2149474448 AC    0010.942e.3b00 13.0.92.160 (default) 0x225e60
                                                   1:4::5c9f (IANA)
                                                   2003:db0:0:5c9e::/64 (IAPD)
10053b2  BE2.500.ip2149466000 AC    0010.942e.3689 13.0.83.175 (default) 0xfdfe0
                                                   1:4::53b1 (IANA)
                                                   2003:db0:0:53b0::/64 (IAPD)
1004c81  BE2.600.ip2149013936 AC    0010.942e.5230 13.0.76.129 (default) 0x4079a0
                                                   1:4::4c80 (IANA)
                                                   2003:db0:0:4c7f::/64 (IAPD)
1004aaa  BE2.500.ip2149353232 AC    0010.942e.3205 13.0.74.169 (default) 0x5192e0
                                                   1:4::4aa9 (IANA)
                                                   2003:db0:0:4aa8::/64 (IAPD)
1004927  BE2.600.ip2149518576 AC    0010.942e.50b1 13.0.73.116 (default) 0x219ba0
                                                   1:4::4926 (IANA)
                                                   2003:db0:0:4925::/64 (IAPD)
10047e4  BE2.800.ip2149422928 AC    0010.9431.a7c7 13.0.71.228 (default) 0x41ff60
                                                   1:4::47e4 (IANA)
                                                   2003:db0:0:47e2::/64 (IAPD)
1004777  BE2.600.ip2149520224 AC    0010.942e.5021 13.0.71.115 (default) 0x41420
                                                   1:4::4776 (IANA)
                                                   2003:db0:0:4775::/64 (IAPD)
1003a6d  BE2.800.ip2149369728 AC    0010.9431.a3a1 13.0.58.105 (default) 0x141360
                                                   1:4::3a6d (IANA)
```

```
                                                    2003:db0:0:3a6a::/64 (IAPD)
10038b7  BE2.600.ip2149362240 AC    0010.942e.4bb2 13.0.56.178 (default) 0x259aa0
                                                    1:4::38b6 (IANA)
                                                    2003:db0:0:38b5::/64 (IAPD)
10028ba  BE2.500.ip2149210768 AC    0010.942e.2873 13.0.40.185 (default) 0x129620
                                                    1:4::28b9 (IANA)
                                                    2003:db0:0:28b8::/64 (IAPD)
100247b  BE2.600.ip2149396320 AC    0010.942e.46a3 13.0.36.113 (default) 0x4b8e0
                                                    1:4::2471 (IANA)
                                                    2003:db0:0:2470::/64 (IAPD)
100207a  BE2.500.ip2149356496 AC    0010.942e.2663 13.0.32.117 (default) 0x1a9460
                                                    1:4::2079 (IANA)
                                                    2003:db0:0:2078::/64 (IAPD)
1001d3f  BE2.600.ip2149251360 AC    0010.942e.44d4 13.0.29.61 (default) 0xcc760
```

-
```
Router#show cnbng-nal subscriber all summary
Sun Aug  2 16:26:44.281 UTC
=====================
Location: 0/RSP0/CPU0
=====================

               Type            PPPoE           IPoE
               ====            =====           ====

Session Counts by State:
        initializing           0               0
          connecting           0               0
           connected           0               0
           activated           0               130
                idle           0               0
       disconnecting           0               0
               Total:          0               130

Session Counts by Address-Family:
               none            0               0
               ipv4            0               130
               ipv6            0               0
               dual            0               0
              Total:           0               130

=====================

   Location: 0/RSP0/CPU0

   =====================
```

```
                  Type         PPPoE       IPoE
                  ====         =====       ====


  Session Counts by State:
         initializing         0           0
           connecting         0           0
            connected         226         0
            activated         31774       0
                 idle         0           0
        disconnecting         0           0
                Total:        32000       0


  Session Counts by Address-Family:
                  none        226         0
                  ipv4        7774        0
                  ipv6        0           0
                  dual        24000       0
                 Total:       32000       0
```

-
```
Router#show cnbng-nal subscriber all detail
Mon Aug  3 00:00:14.624 UTC
Location: 0/2/CPU0
====================
Location: 0/RSP1/CPU0
====================
Interface:                 Bundle-Ether1.1.ip2148413040
UPID:                      0x800e2e70
CPID:                      0x0100918f
PPPOE Session Id:          0x0000
Type:                      IPoE
IPv4 Address:              0.0.0.0
IPv4 Framed Route:
  Prefix:                  0.0.0.0/0
  Next Hop:                0.0.0.0
  Tag:                     0
IPv6 IANA Address:         1:5::345c
IPv6 IAPD Prefix:          2004:cd0:0:188d::/64
CPE link local Address:    ::
IPv6 Framed Route:
  Prefix:                  ::/0
  Next Hop:                ::
  Tag:                     0
IPv6 State:                UP, Sat Jul 25 02:09:55 2020
```

```
Mac Address:               5065.aaab.d864
Inner VLAN ID:             Not Set
Outer VLAN ID:             100
Outer VLAN Cos:            0
Outer VLAN DEI:            1
Created:                   Sat Jul 25 02:09:54 2020
State:                     Activated
Ifhandle:                  0x000b75a0
VRF:                       default
Access-interface:          Bundle-Ether1.1
 Attribute List: 0x5556aed3f878
1:  ipv6-enable     len=  4  value= 1(1)
2:  ipv4-unnumbered len=  9  value= Loopback1
3:  strict-rpf      len=  4  value= 1(1)
4:  ipv6-strict-rpf len=  4  value= 1(1)
5:  ipv4-icmp-unreachable len=  4  value= 1(1)
6:  ipv6-unreachable len=  4  value= 1(1)
7:  ipv4-mtu        len=  4  value= 1500(5dc)
8:  ipv6-mtu        len=  4  value= 1500(5dc)
Session Accounting:        enabled
Interim Interval:          1800 secs
Last interim timestamp:    Sun Aug  2 23:39:46 2020
Interim fail count: None
Last interim failed reason: NA
Last stats:
  BytesIn: 0
  BytesOut: 384570
  BytesInGiga: 0
  BytesOutGiga: 0
Feature IDs activated :
  0x800e2e71
  0x800e2e72
```

-

```
Router#show cnbng-nal subscriber type ipoe summary
Mon Aug  3 00:06:15.032 UTC
=====================
Location: 0/RSP0/CPU0
=====================

                Type            PPPoE           IPoE
                ====            =====           ====

Session Counts by State:
        initializing            0               0
          connecting            0               0
           connected            0               0
           activated            0               8000
                idle            0               0
       disconnecting            0               0
              Total:            0               8000

Session Counts by Address-Family:
                none            0               0
                ipv4            0               0
                ipv6            0               8000
                dual            0               0
              Total:            0               8000

=====================
Location: 0/RSP1/CPU0
=====================
```

```
                Type            PPPoE           IPoE
                ====            =====           ====

Session Counts by State:
        initializing            0               0
          connecting            0               0
           connected            0               0
           activated            0               8000
                idle            0               0
       disconnecting            0               0
               Total:           0               8000

Session Counts by Address-Family:
                none            0               0
                ipv4            0               0
                ipv6            0               8000
                dual            0               0
              Total:            0               8000

Router#
```

-
```
Router#show cnbng-nal subscriber type pppoe summary
Mon Aug  3 00:06:15.032 UTC
=====================
Location: 0/RSP0/CPU0
=====================

                Type            PPPoE           IPoE
                ====            =====           ====

Session Counts by State:
        initializing            0               0
          connecting            0               0
           connected            0               0
           activated            31031           0
                idle            0               0
       disconnecting            0               0
               Total:           31031           0

Session Counts by Address-Family:
                none            0               0
                ipv4            31031           0
                ipv6            0               0
                dual            0               0
              Total:            31031           0

Router#
```

-
```
Router#show cnbng-nal subscriber disconnect-history unique
Mon Aug  3 00:07:22.716 UTC

Location: 0/RSP1/CPU0

| Count|       Last Interface        | Disconnected Reason |            Last Time
                                                                        Disconnected

 Location: 0/1/CPU0
 Location: 0/RSP0/CPU0

| Count|       Last Interface        | Disconnected Reason |            Last Time
                                                                        Disconnected
35494    Bundle-Ether1.1.ip2148328848  Disconnect by CP                 Sat Jul 25
                                                                        02:04:55 2020
```

```
14154    Bundle-Ether1.1.ip2148324096  Disconnect by clear CLI          Sat Jul 25
                                                                        02:05:48 2020

 2777    Bundle-Ether1.1.ip2148194512  Disconnect due to create failure Sat Jul 25
                                                                        01:38:29 2020
```

- ```
  Router#show cnbng-nal subscriber disconnect-history last location
  Mon Aug  3 00:08:42.655 UTC

  Disconnect-reason:         Disconnect by clear CLI
  Disconnect-timestamp:      Sat Jul 25 02:05:48 2020
    Message Txn ID: 55663
    Session Txn ID: 1
    Failed at: Sat Jul 25 01:57:03 2020
    Feature Mask: 0x0
    SVM State: 0
    IPSUB flags: 0x600a200
    Pending callback: 0x2
    Data:

  Interface:                 Bundle-Ether1.1.ip2148324096
  UPID:                      0x800cd300
  CPID:                      0x01007bd8
  PPPOE Session Id:          0x0000
  Type:                      IPoE
  IPv4 Address:              0.0.0.0
  IPv4 Framed Route:
    Prefix:                  0.0.0.0/0
    Next Hop:                0.0.0.0
    Tag:                     0
  IPv6 IANA Address:         1:5::3de5
  IPv6 IAPD Prefix:          2004:cd0:0:616::/64
  CPE link local Address:    ::
  IPv6 Framed Route:
    Prefix:                  ::/0
    Next Hop:                ::
    Tag:                     0
  IPv6 State:                UP, Sat Jul 25 01:57:03 2020
  Mac Address:               5065.aaab.cfbb
  Inner VLAN ID:             Not Set
  Outer VLAN ID:             100
  Outer VLAN Cos:            0
  Outer VLAN DEI:            1
  Created:                   Sat Jul 25 02:05:48 2020
  State:                     Init
  Ifhandle:                  0x000323a0
  VRF:                       default
  Access-interface:          Bundle-Ether1.1
   Attribute List: 0x559125764408
  1:  ipv6-enable     len=  4  value= 1(1)
  2:  ipv4-unnumbered len=  9  value= Loopback1
  3:  strict-rpf      len=  4  value= 1(1)
  4:  ipv6-strict-rpf len=  4  value= 1(1)
  5:  ipv4-icmp-unreachable len=  4  value= 1(1)
  6:  ipv6-unreachable len=  4  value= 1(1)
  7:  ipv4-mtu        len=  4  value= 1500(5dc)
  8:  ipv6-mtu        len=  4  value= 1500(5dc)
  Session Accounting:        enabled
  Interim Interval:          1800 secs
  Last interim timestamp:    Sat Jul 25 02:05:47 2020
  Interim fail count: None
  Last interim failed reason: NA
  ```
  ```

```
Last stats:
  BytesIn: 0
  BytesOut: 540
  BytesInGiga: 0
  BytesOutGiga: 0
Feature IDs activated :
  0x800cd301
  0x800cd302

[Event History]
UPID:  0x800cd300

| Event Name               | Time Stamp             | S, M
| Create                   | Jul 25 01:57:02.999679 | 0, 0
| New Session Request      | Jul 25 01:57:02.999686 | 0, 0
| Interface create         | Jul 25 01:57:02.999823 | 0, 0
| SVM create               | Jul 25 01:57:03.018268 | 0, 0
| UP Install(req)          | Jul 25 01:57:03.018321 | 0, 0
| UP Install(CB)           | Jul 25 01:57:03.019220 | 0, 0
| Last Assoc(req)          | Jul 25 01:57:03.019232 | 0, 0
| Last Assoc(CB)           | Jul 25 01:57:03.020160 | 0, 1
| Produce done(req)        | Jul 25 01:57:03.020233 | 0, 0
| IPv4 Caps Up             | Jul 25 01:57:03.188034 | 0, 0
| IPv6 Caps Up             | Jul 25 01:57:03.233210 | 0, 0
| Init data req            | Jul 25 01:57:03.254482 | 0, 1
| Init data cb             | Jul 25 01:57:03.369027 | 0, 1
| Client Session up        | Jul 25 01:57:03.379152 | 0, 0
| Produce done             | Jul 25 01:57:03.977629 | 0, 0
| IPv6 Up                  | Jul 25 01:57:03.977643 | 0, 0
| Session up notified      | Jul 25 01:57:03.977650 | 0, 0
| Stats start              | Jul 25 01:57:03.977841 | 0, 0
| Disconnect notified      | Jul 25 02:05:47.548202 | 0, 0
| Disconnect ack           | Jul 25 02:05:47.550293 | 0, 0
| IPv4 Caps Down           | Jul 25 02:05:47.652232 | 0, 0
| IPv6 Caps Down           | Jul 25 02:05:47.652333 | 0, 0
| Final stats              | Jul 25 02:05:47.753805 | 0, 0
| SVM delete               | Jul 25 02:05:47.780713 | 0, 0
| SVM cleanup              | Jul 25 02:05:48.283050 | 0, 0
Help: S - Sticky Event, M - Multiple Occurrence
```

-

```
Router#show cnbng-nal subscriber fadb
Mon Aug  3 00:03:12.858 UTC

Location: 0/RSP1/CPU0
==================

UPID:       0x800ec810
Service-ID: 0x04000003  Service-Name: JHV_VOICE
Feature-ID: 0x800ec812
 Attribute List: 0x559cba6d0008
1:  feature-acct-bitmask len=  4  value= 805306413(3000002d)
Accounting:               enabled
Interim fail count: None
Last interim failed reason: None
Last stats:
  BytesIn: 0
  BytesOut: 0
  BytesInGiga: 0
  BytesOutGiga: 0

UPID:       0x800e9470
Service-ID: 0x04000003  Service-Name: JHV_VOICE
```

```
Feature-ID: 0x800e9472
 Attribute List: 0x559cba6d0008
1:  feature-acct-bitmask len=  4  value= 805306413(3000002d)
Accounting:               enabled
Interim fail count: None
Last interim failed reason: None
Last stats:
  BytesIn: 0
  BytesOut: 0
  BytesInGiga: 0
  BytesOutGiga: 0

UPID:       0x800e7ee0
Service-ID: 0x04000003  Service-Name: JHV_VOICE
Feature-ID: 0x800e7ee2
 Attribute List: 0x559cba6d0008
1:  feature-acct-bitmask len=  4  value= 805306413(3000002d)
Accounting:               enabled
Interim fail count: None
Last interim failed reason: None
Last stats:
  BytesIn: 0
  BytesOut: 0
  BytesInGiga: 0
  BytesOutGiga: 0

UPID:       0x800e16e0
Service-ID: 0x04000004  Service-Name: LIVE_TV
Feature-ID: 0x800e16e1
 Attribute List: 0x559cba6d0008
1:  feature-acct-bitmask len=  4  value= 0(0)
Accounting:               disabled
Interim fail count: None
Last interim failed reason: None
Last stats:
  BytesIn: 0
  BytesOut: 0
  BytesInGiga: 0
  BytesOutGiga: 0

UPID:       0x800dda90
Service-ID: 0x04000003  Service-Name: JHV_VOICE
Feature-ID: 0x800dda91
 Attribute List: 0x559cba6d0008
1:  feature-acct-bitmask len=  4  value= 805306413(3000002d)
Accounting:               enabled
Interim fail count: None
Last interim failed reason: None
Last stats:
  BytesIn: 0
  BytesOut: 0
  BytesInGiga: 0
  BytesOutGiga: 0

UPID:       0x800dd4e0
Service-ID: 0x04000004  Service-Name: LIVE_TV
Feature-ID: 0x800dd4e1
 Attribute List: 0x559cba6d0008
1:  feature-acct-bitmask len=  4  value= 0(0)
Accounting:               disabled
Interim fail count: None
Last interim failed reason: None
Last stats:
  BytesIn: 0
```

```
  BytesOut: 0
  BytesInGiga: 0
  BytesOutGiga: 0
```

Verify cnBNG NAL Counters

You can use the following commands to verify various NAL counters on the cnBNG user plane:

-

```
Router#show cnbng-nal counters type all
Sun Aug  2 20:42:49.548 UTC

Location: 0/RSP0/CPU0

Subscriber Counters
-------------------

Counter name                      Value
============                      =====
INTF Delete                       500
IPv4 caps down                    500
IPv6 caps down                    500
IPv4 Rou del                      500
IPv6 Rou del                      500
Blkdis q empty                    1
DB cache hit                      17113

Error Counters
--------------

Counter name                      Value
============                      =====

Accounting Counters
-------------------

Counter name                      Value
============                      =====
Sess Stop req                     500
Feat Stop req                     500
Stop req                          3000
Stop cb                           3000
Final cb                          3000
Feat Final cb                     500
Sess Final cb                     2500

SVM Counters
------------

Counter name                      Value
============                      =====
Sess deleted                      500
Delete CB                         500
Feat deleted                      1000
Cleanup                           500
Sess stats, before svm            500
Feat stats, before svm            500

SPA Counters
------------
```

```
Counter name                        Value
=============                       =====
SPA Delete Req                      500
SPA Update Req                      500
Sub Delete Res                      500
Sub Update Res                      500
Blkdic adm more                     39
GTPu pkt sent                       1000
PFCP pkt sent                       1463
GTPu pkt punt                       500
PFCP pkt punt                       1463
DHCPv4 pkt punt                     500
DHCPv6 pkt punt                     500
DHCPv6 pkt inj                      500
Alloc count                         3463
Free count                          3463
Mutex lock                          6741
Mutex unlock                        6741
Timer start                         463
Timer expiry                        463
Sub Update IPOE OK                  500
Sub Delete IPOE OK                  500

CP Recon Counters
------------------

Counter name                        Value
=============                       =====

Histogram/API Performance Stats
--------------------------------

API name       1ms       10ms  100ms  1s  5s  10s  20s  50s  100s
========       ===       ====  =====  ==  ==  ===  ===  ===  ====
Per trans      410       90    0      500 0   0    0    0    0
Sub Create     0         0     0      0   0   0    0    0    0
Sub Update     445       55    0      0   0   0    0    0    0
Sub Delete     0         0     0      500 0   0    0    0    0
IPOE Int Crt   0         0     0      0   0   0    0    0    0
IPOE Int Upd   0         0     0      0   0   0    0    0    0
IPOE Int Del   0         0     0      500 0   0    0    0    0
PPPOE Int Crt  0         0     0      0   0   0    0    0    0
PPPOE Int Upd  0         0     0      0   0   0    0    0    0
PPPOE Int Del  0         0     0      0   0   0    0    0    0
Sess Create    0         0     0      0   0   0    0    0    0
Sess Update    0         0     0      0   0   0    0    0    0
Sess Delete    0         0     10     490 0   0    0    0    0
V4 RT Inst     0         0     0      0   0   0    0    0    0
V4 RT Del      0         6     320    174 0   0    0    0    0
V4 FR Inst     0         0     0      0   0   0    0    0    0
V4 FR Del      0         0     0      0   0   0    0    0    0
V6 RT Inst     0         0     0      0   0   0    0    0    0
V6 RT Del      0         6     310    184 0   0    0    0    0
V6 PD RT Inst  0         0     0      0   0   0    0    0    0
V6 PD RT Del   0         0     0      0   0   0    0    0    0
V6 FR Inst     0         0     0      0   0   0    0    0    0
V6 FR Del      0         0     0      0   0   0    0    0    0
CDM Lookup     0         0     0      0   0   0    0    0    0
CDM Insert     0         0     0      0   0   0    0    0    0
CDM Update     1469      31    0      0   0   0    0    0    0
Eval Lookup    0         0     0      0   0   0    0    0    0
```

-
```
Router#show cnbng-nal counters type all | beg SPA LIB
Sun Aug  2 20:44:07.902 UTC
SPA LIB Counters
----------------

Counter name                      Value
=============                     =====
pfcp_rx_counter                   6899
pfcp_tx_counter                   6900
gtpu_tx_counter                   9048
gtpu_rx_counter                   7510
pfcp_keepalive_tx_counter         891
pfcp_keepalive_rx_counter         890

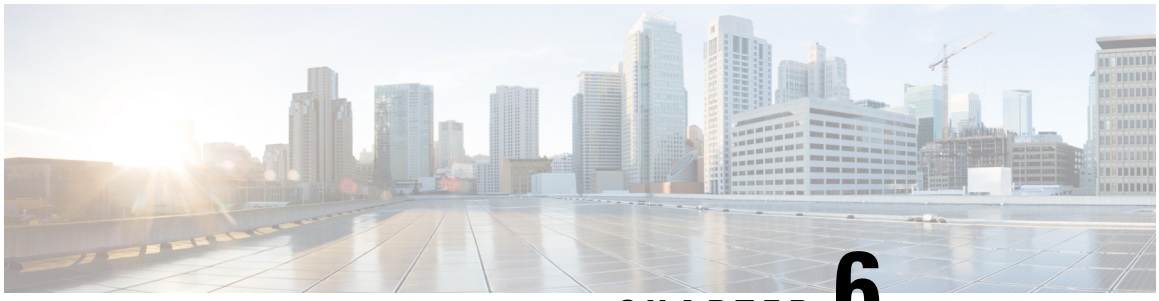
SPA API counters
----------------------
```

-
```
Router#show cnbng-nal counters type spa
Sun Aug  2 20:42:13.703 UTC

Location: 0/RSP0/CPU0

SPA Counters
------------

Counter name                      Value
=============                     =====
SPA Delete Req                    500
SPA Update Req                    500
Sub Delete Res                    500
Sub Update Res                    500
Blkdic adm more                   39
GTPu pkt sent                     1000
PFCP pkt sent                     1461
GTPu pkt punt                     500
PFCP pkt punt                     1461
DHCPv4 pkt punt                   500
DHCPv6 pkt punt                   500
DHCPv6 pkt inj                    500
Alloc count                       3461
Free count                        3461
Mutex lock                        6727
Mutex unlock                      6727
Timer start                       461
Timer expiry                      461
Sub Update IPOE OK                500
Sub Delete IPOE OK                500
```



CHAPTER 6

Subscriber Management

This chapter provides information about various types of subscriber sessions, namely IPoE and PPPoE, and IP addressing by DHCP. Also, on how the point-point frames are tunnelled across the network using the Layer 2 Tunneling Protocol.

Subscriber Session Overview

To enable subscribers to access the network resources, the network has to establish a session with the subscriber. A subscriber session represents the logical connection between the customer premise equipment (CPE) and the network resource. Each session establishment comprises the following phases:

- Establishing a connection—in this phase CPE finds the cnBNG with which to communicate.
- Authenticating and authorizing the subscriber—in this phase, cnBNG authenticates the subscribers and authorizes them to use the network. This phase is performed with the help of the RADIUS server.
- Giving the subscriber an identity—in this phase, the subscriber is assigned an identity, the IP address.
- Monitoring the session—in this phase, cnBNG ascertains that the session is up and running.

The subscriber sessions are established over the subscriber interfaces, which are virtual interfaces. It's possible to create only one interface for each subscriber session. A port can contain multiple VLANs, each of which can support multiple subscribers. cnBNG creates subscriber interfaces for each kind of session. These interfaces are named based on the parent interface, such as bundle-ether 2.100.pppoe312. The subscribers on bundle interfaces (or bundle-VLANs) allow redundancy and are managed on the cnBNG route processor (RP).

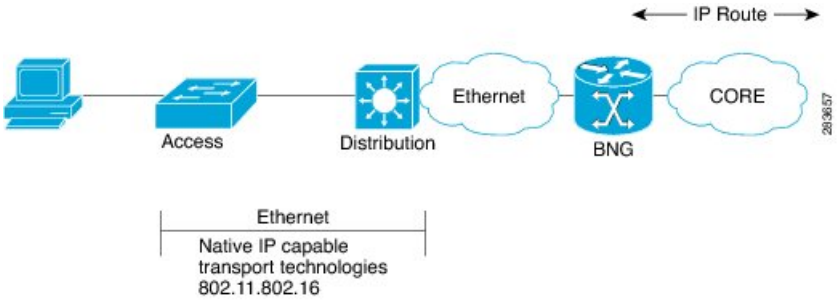
There are two mechanisms to establish a subscriber session, namely, IPoE Session and PPP over Ethernet (PPPoE).

IPoE Session

In an Internet over Ethernet (IPoE) subscriber session, subscribers run IPv4 or IPv6 on the CPE device and connect to the cnBNG through a Layer-2 aggregation. IP subscriber sessions that connect through a Layer-2

aggregation network are called L2-connected. IPoE subscriber sessions are always terminated on cnBNG and then routed into the service provider network. IPoE relies on DHCP to assign the IP address.

Figure 8: IPoE Session



cnBNG supports both DHCP v4 and DHCP v6 subscriber sessions.

Limitations

The following are the limitations:

- L3 routed subscribers are not supported.
- Geo redundancy or subscriber redundancy is not supported.
- Line card or physical port termination-based subscribers are not supported.

Configuration Example

```
Router#configure
Router(config)#interface Bundle-Ether1.1
Router(config-subif)#ipv4 point-to-point
Router(config-subif)#ipv4 unnumbered Loopback1
Router(config-subif)#ipv6 enable
Router(config-subif)#encapsulation dot1q 1
Router(config-subif)#ipsubscriber
Router(config-cnbng-nal-ipsub)#ipv4 l2-connected
Router(config-cnbng-nal-ipsub-l2conn)#initiator dhcp
Router(config-cnbng-nal-ipsub-l2conn)#exit
Router(config-cnbng-nal-ipsub)#ipv6 l2-connected
Router(config-cnbng-nal-ipsub-ipv6-l2conn)#initiator dhcp
Router(config-cnbng-nal-ipsub-ipv6-l2conn)#commit
```

Running Configuration

```
Router#show running-config interface be1.1
interface Bundle-Ether1.1
 ipv4 point-to-point
 ipv4 unnumbered Loopback1
 ipv6 enable
 encapsulation dot1q 1
 ipsubscriber
  ipv4 l2-connected
   initiator dhcp
  !
  ipv6 l2-connected
   initiator dhcp
```

!
!

PPP over Ethernet (PPPoE)

The Point-to-Point Protocol (PPP) is used for communications between two nodes, like a client and a server. The PPP provides a standard method for transporting multiprotocol datagrams over point-to-point links. It defines an encapsulation scheme, a link layer control protocol (LCP), and a set of network control protocols (NCPs) for different network protocols that can be transmitted over the PPP link.

One of the methods to establish PPP connection is by the use of PPPoE. In a PPPoE session, the PPP protocol runs between the CPE and cnBNG. The Home Gateway (which is part of the CPE) adds a PPP header (encapsulation) that is terminated at the cnBNG.

PPPoE Discovery

The PPPoE discovery-stage protocol consists of basic packet exchange between the subscriber and server (cnBNG). The following is the list of the various PPPoE Active Discovery (PAD) messages:

- PPPoE Active Discovery Initiation (PADI)—The CPE broadcasts to initiate the process to discover cnBNG.
- PPPoE Active Discovery Offer (PADO)—The cnBNG responds with an offer.
- PPPoE Active Discovery Request (PADR)—The CPE requests to establish a connection.
- PPPoE Active Discovery Session confirmation (PADS)—cnBNG accepts the request and responds by assigning a session identifier (Session-ID).
- PPPoE Active Discovery Termination (PADT)—Either CPE or cnBNG terminates the session.

PPoE Sessions

The PPPoE sessions are of the following types:

- PPPoE PPP Terminated sessions Terminated (PTA)
- PPPoE L2TP Access Concentrator Sessions (LAC)
- L2TP Network Server Sessions (LNS)

Majority of the digital subscriber line (DSL) broadband deployments use Point-to-Point Protocol over Ethernet (PPPoE) sessions to provide subscriber services. These sessions terminate the Point-to-Point Protocol (PPP) link and provide all the features, service, and billing on the same node. These sessions are called PPP Terminated (PTA) sessions. See PPPoE PPP Terminated and Aggregation Sessions (PPPoE-PTA), on page 56.

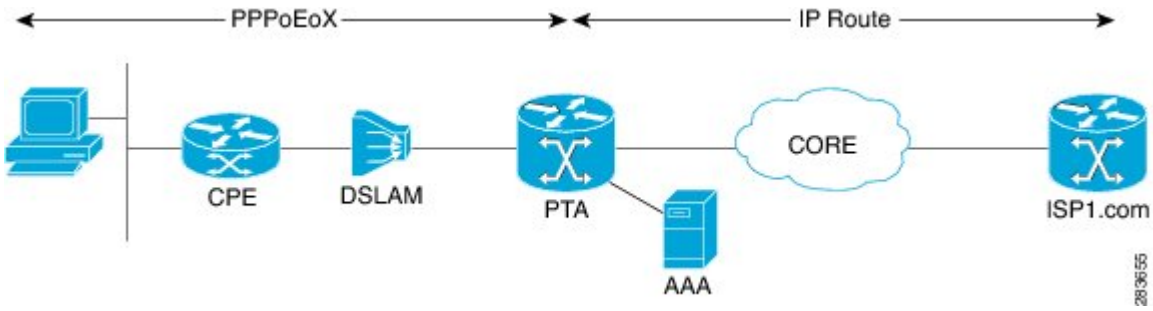
There are some wireline subscriber deployments in the wholesale retail model where ISPs work with others to provide the access and core services separately. In such cases, the subscribers are tunneled between wholesale and retail ISPs using the Layer 2 Tunneling Protocol (L2TP), a client-server protocol. See L2TP Access Concentrator Sessions (LAC), on page 57 and L2TP Network Server Sessions (LNS), on page 61.

Note For the functioning of PPP PTA and PPP LAC session, the RADIUS server must be set up to authenticate and forward sessions as necessary. There's no local authentication available on cnBNG.

PPPoE PPP Terminated and Aggregation Sessions (PPPoE-PTA)

In a PPPoE-PPP Termination and Aggregation (PTA) session, the PPP encapsulation is terminated on cnBNG. After it's terminated, cNBNG routes the traffic to the service provider using IP routing. A typical PTA session is depicted in this figure.

Figure 9: PPPoE-PTA Session



PPPoE session configuration information is contained in PPPoE profiles. After a profile is defined, it's assigned to an access interface. Multiple PPPoE profiles can be created and assigned to multiple interfaces. A global PPPoE profile can also be created; the global profile serves as the default profile for any interface that has not been assigned a specific PPPoE profile.

The PPP PTA session is typically used in the Network Service Provider (retail) model where the same service operator provides the broadband connection to the subscriber and also manages the network services.

Limitations

The following are the limitations:

- L3 routed subscribers are not supported.
- Geo redundancy or subscriber redundancy is not supported.
- Line card or physical port termination-based subscribers aren't supported.

Configure PPPoE-PTA Session

The following section describes the steps to configure PPPoE-PTA sessions:

- Configure the access-interface
- Enable PPPoE

Configuration Example

```
Router#configure
Router(config)#interface Bundle-Ether1.1
Router(config-subif)#ipv4 point-to-point
Router(config-subif)#ipv4 unnumbered Loopback1
Router(config-subif)#ipv6 enable
Router(config-subif)#encapsulation dot1q 1

/* Enable PPPoE */
```

```
Router(config-subif)#pppoe enable
Router(config-subif)#commit
```

Running Configuration

```
Router#show running-config interface be1.1
interface Bundle-Ether1.1
 ipv4 point-to-point
 ipv4 unnumbered Loopback1
 ipv6 enable
 encapsulation dot1q 1

 pppoe enable
!
```

L2TP Access Concentrator Sessions (LAC)

Table 5: Feature History Table

Feature Name	Release Information	Feature Description
Enable LAC on Cloud Native BNG	Release 7.4.2	This feature enables the cloud native BNG user plane to become an L2TP access concentrator (LAC), allowing you to tunnel point-to-point frames between the remote system or LAC client and an LNS located at a wholesaler. This functionality provides highly flexible deployments options to suit different customer use-cases and needs. To enable this feature, use the **l2tp enable** command.

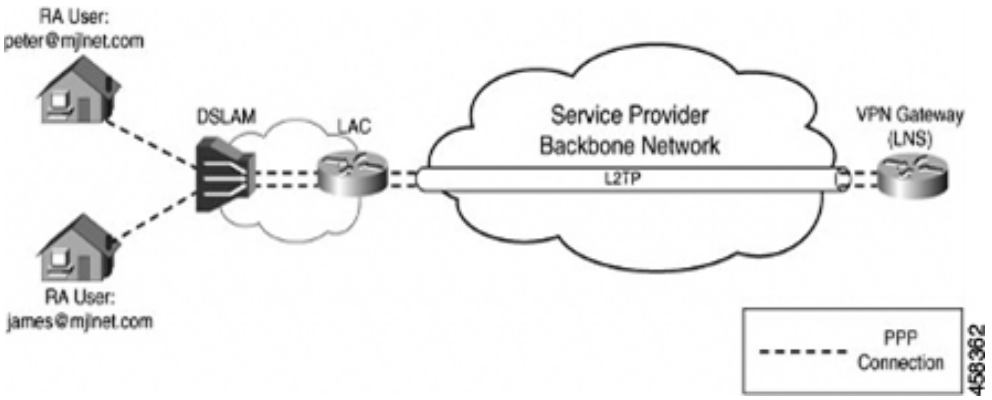
L2TP encapsulates and tunnels the PPP Layer 2 frames through a Layer 3 network. With L2TP, you can have a layer 2 connection to an access concentrator. The concentrator then tunnels individual PPP frames to the Network Access Server (NAS). This allows the processing of PPP packets on different devices. L2TP can be used to make all multilink channels terminate at a single NAS. Thus-allowing multilink operation even when the calls are spread across distinct physical NASs.

In cnBNG, L2TP uses the following two components to perform the hand-off task of the subscriber traffic to the Internet service provider (ISP).

- L2TP Access Concentrator (LAC)—The L2TP enables subscribers to dial into the LAC, which extends the PPP session to the LNS. cnBNG provides LAC.
- L2TP Network Server (LNS)—The L2TP extends PPP sessions over an arbitrary network to a remote network server that is, the LNS. The ISP provides LNS.

The following image depicts the overall topology of LAC and LNS:

Figure 10: Topology of LAC and LNS



The remote user initiates a PPP connection across the cloud to a LAC. The LAC acts as a client and then tunnels the PPP connection across the Internet to an LNS that acts as a server.

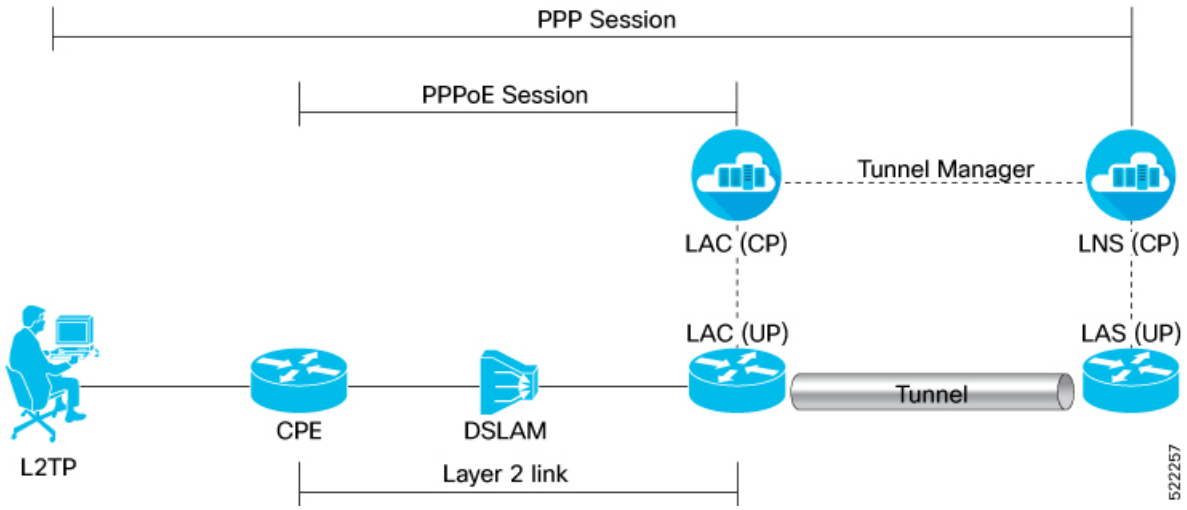
L2TP utilizes two types of messages, control messages and data messages. Control messages are used in the establishment, maintenance, and clearing of tunnels and calls. Data messages are used to encapsulate PPP frames over the tunnel.

```
+--------------------+
| PPP Frames         |
+--------------------+    +-----------------------+
| L2TP Data Messages|    | L2TP Control Messages |
+--------------------+    +-----------------------+
| L2TP Data Channel |    | L2TP Control Channel  |
| (unreliable)      |    | (reliable)            |
+-------------------------------------------------+
|      Packet Transport (UDP, FR, ATM)     |
+-------------------------------------------------+
```

PPP frames are passed over an unreliable data channel that is encapsulated first by an L2TP header. Then a Packet Transport such as UDP. Control messages are sent over a reliable L2TP Control Channel, which transmits packets in-band over the same Packet Transport.

During a PPP LAC session, the PPPoE encapsulation terminates on cnBNG; however, the PPP packets travel beyond cnBNG to LNS through the L2TP tunnel. A typical LAC session is depicted in the following figure.

Figure 11: LAC Session



Both LAC and LNS sessions use L2TP protocol for negotiation and creation of L2TP sessions.

For more information on the LAC high-level work flow, see the *L2TP Subscriber Management* chapter in the *Cloud Native BNG Control Plane Configuration Guide*.

The PPP LAC session is used in the wholesaler model, where the network service provider is a separate entity from the local access network provider. In this kind of setup, the access network provider owns the LAC and the network service provider owns the LNS.

- Network service provider performs access authentication, manage and provide IP addresses to subscribers, and are responsible for overall service.
- The access network prover is responsible for providing the last-mile digital connectivity to the customer, and for passing on the subscriber traffic to the service provider.

Limitations for LAC Sessions

The following are the limitations for the LAC sessions:

- Tunnel specific statistics are not supported.
- LAC and LNS cannot coexist on the same node.
- IPv6 L2TP tunnel is not supported.
- L2TP tunnel keep alive or hello packet offload is not supported.
- Setting of type of service is not supported.
- Multicast group is not supported.
- L2TP packet segmentation or reassemble is not supported.
- The following features aren’t supported:
  - Access Control List (ACL)

- Quality of Service (QoS)
- Policy-based Routing (PBR)
- Unicast Reverse Path Forwarding (uRPF)
- ICMP unreachable

Configure LAC Sessions

This section describes how to configure the LAC session on the cnBNG user plane.

- Enable L2TP
- Establish PPPoE connection

Configuration Example

Enable L2TP:

```
Router#configure
Router(config)#cnbng-nal location 0/1/CPU0

Router(config-cnbng-nal-local)#hostidentifier RTR1

Router(config-cnbng-nal-local)#up-server ipv4 192.0.2.1 gtp-port 15002 pfcp-port 15003
vrf default
Router(config-cnbng-nal-local)#cp-server primary ipv4 198.51.100.1

Router(config-cnbng-nal-local)#enable-test-server

Router(config-cnbng-nal-local)#disconnect-history file-logging-enable

Router(config-cnbng-nal-local)#cp-association retry-count 5

Router(config-cnbng-nal-local)#l2tp enable

Router(config-cnbng-nal-local)#l2tp-tcp-mss-adjust 1400
```

Establish PPPoE connection:

```
Router(config-cnbng-nal-local)#interface Bundle-Ether1.1

Router(config-subif)#ipv4 address 192.11.1.1 255.255.255.0

Router(config-subif)#ipv6 enable

Router(config-subif)#encapsulation dot1q 1

Router(config-subif)#ppoe enable
Router(config-subif)#commit
Router(config-subif)#exit
Router(config)#exit
```

Running Configuration

```
Router#show running-config

cnbng-nal location preconfigure 0/1/CPU0
 l2tp-tcp-mss-adjust 1400
 hostidentifier RTR1
 up-server ipv4 192.0.2.1 gtp-port 15002 pfcp-port 15003 vrf default
 cp-server primary ipv4 198.51.100.1
 disconnect-history file-logging-enable
 cp-association retry-count 5
 l2tp enable
 enable-test-server
!
interface Bundle-Ether1
!
interface Bundle-Ether1.1
 ipv4 address 192.11.1.1 255.255.255.0
 ipv6 enable
 encapsulation dot1q 1
 pppoe enable
!
```

L2TP Network Server Sessions (LNS)

Table 6: Feature History Table

Feature Name	Release Information	Feature Description
Enable LNS on Cloud Native BNG	Release 7.4.2	This feature enables cloud native BNG (cnBNG) to act as an L2TP Network Server (LNS) located at the wholesaler and allows you to terminate the tunnel or the subscriber sessions initiated by the LAC client. The cnBNG LNS solution offers control and user plane separation (CUPS) and cloud-native advantages for next-generation subscriber services in operator networks where subscribers connect directly to a retailer. To enable this feature, use the **lns enable** command.

L2TP Network Server (LNS) resides at one end of an L2TP tunnel and acts as a peer to the LAC. An LNS acts like an L2TP server that terminates the incoming tunnel from the L2TP LAC. An LNS is the logical termination point of the PPP session that is being tunneled from the client by the LAC.

LNS sessions are similar to PTA sessions in the overall functionality. Instead of the PPPoE protocol, here the First-Sign-Of-Life (FSOL) packets are the L2TP Incoming-Call-Request (ICRQ) messages.

For more information on the LNS high-level workflow, see the *L2TP Subscriber Management* chapter in the *Cloud Native BNG Control Plane Configuration Guide*.

Limitations for LNS Sessions

The following are the limitations for the LNS sessions:

- IPv6 L2TP tunnel is not supported.
- L2TP tunnel keep alive or hello packet offload is not supported.
- Tunnel statistics are not supported.
- Termination on non bundle-ether is not supported (for example, PWHE, physical interface).
- Termination of the VLAN interface is not supported.
- Supports parent interface only and not subinterface.
- L2TP packet segmentation or reassemble is not supported.
- Parent interface SVLAN policy must be different for other interfaces on the chassis.
- The following features are not supported:
  - Unicast Reverse Path Forwarding (uRPF)
  - Lawful Intercept (LI)

Configure LNS Sessions

This section describes how to configure the LNS session on the cnBNG user plane.

Configuration Example

To enable L2TP:

```
Router#configure
Router(config)#cnbng-nal location 0/0/CPU0
Router(config-cnbng-nal-local)#hostidentifier RTR1
Router(config-cnbng-nal-local)#up-server ipv4 192.0.2.1 gtp-port 15002 pfcp-port 15003
vrf default
Router(config-cnbng-nal-local)#cp-server primary ipv4 198.51.100.1
Router(config-cnbng-nal-local)#enable-test-server
Router(config-cnbng-nal-local)#disconnect-history file-logging-enable
Router(config-cnbng-nal-local)#cp-association retry-count 5
Router(config-cnbng-nal-local)#l2tp enable << Enble L2TP
Router(config-cnbng-nal-local)#commit
Router(config-cnbng-nal-local)#exit
Router(config)#
```

To establish the LNS session:

```
Router(config)#interface bundle-ether 1.1
Router(config-subif)#service-policy output SVLAN subscriber-parent subscriber-group
resourceid 4 << To allow maximum capacicty on the linecard
Router(config-subif)#ipv4 address 192.5.1.1 255.255.255.0
Router(config-subif)#ipv6 enable
```

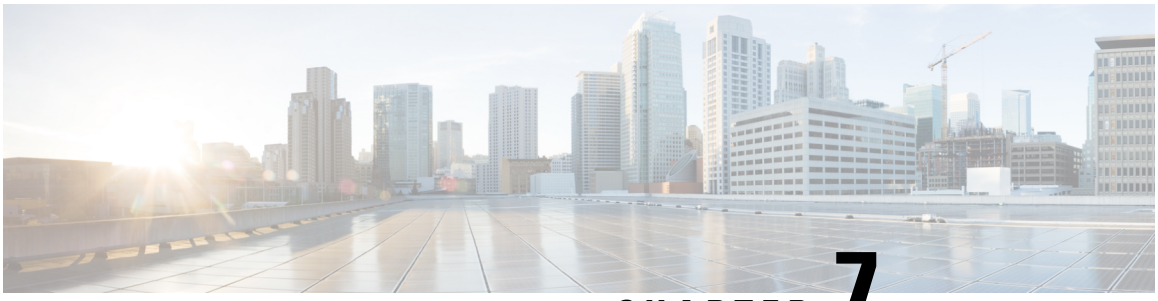
```
Router(config-subif)#lns enable << Establish LNS session
Router(config-subif)#commit
Router(config-subif)#exit
```

Note To allow maximum capacity on the linecard, we recommend you to use the **service-policy output SVLAN subscriber-parent subscriber-group resourceid** command in the main interface.

Running Configuration

```
Router#show running-config

cnbng-nal location preconfigure 0/0/CPU0
 hostidentifier RTR1
 up-server ipv4 192.0.2.1 gtp-port 15002 pfcp-port 15003 vrf default
 cp-server primary ipv4 198.51.100.1
 disconnect-history file-logging-enable
 cp-association retry-count 5
 l2tp enable
 enable-test-server
!
interface Bundle-Ether1.1
 service-policy output SVLAN subscriber-parent subscriber-group resourceid 4
 ipv4 address 192.11.1.1 255.255.255.0
 ipv6 enable
 lns enable
!
```



CHAPTER 7

End-to-End Flow Control

There are various scenarios that might generate sudden spike in the traffic that goes to the cnBNG control plane (CP). To handle these spikes in traffic, it is necessary to flow control and rate limit the CP ingress to ensure that service applications are not overwhelmed with these bursts. The end-to-end flow control feature optimizes flow control and rate limit of the traffic toward the CP ingress. This chapter covers the end-to-end flow control feature on cnBNG user plane (UP).

For details on end-to-end flow control functionality on cnBNG CP, see the *End-to-End Flow Control* chapter in the *Cloud Native BNG Control Plane Configuration Guide*.

End-to-End Flow Control

Table 7: Feature History Table

Feature Name	Release Information	Feature Description
End-to-End Flow Control Between User Plane and Control Plane	Release 7.4.2	In cloud native BNG (cnBNG) networks, this feature allows you to define the rate at which the user plane (UP) sends messages, such as control packets and data packet notifications, to the control plane (CP). The feature regulates the CP ingress traffic flow at the source-of-origin (UP), helping avoid network congestion and packet loss. The feature introduces these commands: • ipoe fsol-flow-control • pppoe fsol-flow-control • up-cp-notification flow-control • up-cp-stats flow-control

The Cloud Native Broadband Network Gateway (cnBNG) manages residential subscribers from different access planes in a centralized way. It accepts and identifies subscriber control plane (CP) traffic coming from multiple user planes (UPs) associated with the CP. When the number of UPs scale, the amount of traffic that eventually reaches the CP from each UP also multiplies.

There are various scenarios where the traffic flow between the CP and UP must be regulated. This regulation is to ensure that the CP attends all the service requests without service interruption. The scenarios that create burst or higher flow rates in the traffic flows are as follows:

- Power outage in a residential area
- Access network outage for a specific period
- Catastrophic events like process crash, route processor reboot, chassis reload, and so on, on UP

These scenarios generate a sudden spike in the traffic going to the CP and it is necessary to use flow control functionality to handle such spikes. The end-to-end flow control feature optimizes the flow control and rate limit of the traffic toward the CP ingress. The feature thus ensures that the service applications are not overwhelmed with traffic bursts.

How it Works

There are two types of traffic that enter or exit the CP—the control traffic that is responsible for subscriber session creation and the control traffic on a subscriber session that is already provisioned. The application infrastructure (App-Infra) features such as Dispatcher and Overload Control, facilitate the cnBNG CP ingress packet flow control. For details on end-to-end flow control functionality on cnBNG CP, see the *End-to-End Flow Control* chapter in the *Cloud Native BNG Control Plane Configuration Guide*.

On the UP side, the end-to-end flow control feature allows you to define the rate at which packet notifications from the UP reach the CP. The protocol packets from CPE, and messages such as statistics and notification events that are locally generated on the UP are subjected to this flow control such that the number of messages reaching the CP are controlled at the source-of-origin itself.

The cnBNG UP provides flow control functionality for the following packets:

- Protocol packets from CPE which include:
  - IPoE DHCPv4 DISCOVER rate control from UP to CP
  - IPoE DHCPv6 SOLICIT rate control from UP to CP
  - PPPoE-PTA (PPP Termination and Aggregation) or LAC (L2TP Access Concentrator) PADI (PPPoE Active Discovery Initiation) rate control from UP to CP
  - PPPoE-PTA DHCPV6 SOLICIT rate control from UP to CP
- Locally generated messages on UP (these messages are common for IPoE, PPPoE-PTA, and PPPoE-LAC):
  - Subscriber delete notification (say, during mark-and-sweep procedure, session deletion by UP administrator, and so on)
  - PPP keep alive timer expiry notification
  - Periodic subscriber session or service statistics notification
- DHCP packets:
  - Network processing unit-level (NPU-level) local packet transport service (lpts) flow control for DHCP broadcast packets
- PPPoE packets:
  - NPU-level lpts flow control for PADI broadcast packets

Based on these packet types, we broadly classify the flow control functionality on UP into:

- UP protocol packet punt flow control
- UP notifications events flow control, which includes:
  - UP delete notification flow control
  - UP statistics report flow control

You can use specific commands on UP to set various flow control limits that define the number of messages sent from UP to CP for each second. The excessive messages are queued up with a limited queue size. The maximum packet holding in the queue is 64K messages. For command details, see the *Configuration* section.

Restrictions

End-to-end flow control feature is applicable only for L2-connected topology—where the DHCP client is connected to cnBNG UP through a direct link, without a relay agent being present in between them. Whereas the feature is not applicable for a relay chaining topology—where a lightweight DHCPv6 relay agent (LDRA) is present in between the DHCP client and the cnBNG UP node. This is because, the cnBNG UP does not perform full packet decoding to identify the SOLICT or DISCOVER packets in such scenarios.

Configure End-to-End Flow Control on cnBNG User Plane

End-to-end flow control configuration on cnBNG UP involves these high-level tasks:

- UP protocol packet punt flow control, using the **fsol-flow-control** command.
- UP notifications events flow control, which includes:
  - UP delete notification flow control, using the **up-cp-notification flow-control** command.
  - UP statistics report flow control, using the **up-cp-stats flow-control** command.

Guidelines for Enabling End-to-End Flow Control Feature

Enabling end-to-end flow control feature is subjected to these guidelines:

- With the flow control feature applied, you might experience packet loss in the following high availability (HA) scenarios such as *cnbng-nal* process restart, RP failover, *cnbng-nal* SMU activation, and bring down of CP-UP association.
- The queue size of the flow control packet is limited to 64K messages due to memory constraints. If the queue is already full, UP drops the new packets.
- To ensure a robust system performance, you must choose the configuration parameters for the flow control feature based on your network topology and bandwidth requirement.
- Refer the *Cloud Native BNG Control Plane Configuration Guide* for details on various flow control configuration parameters on CP.

Configuration Example

- **UP protocol packet punt packet flow control:**

  The UP protocol packet punt flow control limit ranges from 50 to 400 packets for each second, the default being 100.

```
Router#configure
Router(config)#cnbng-nal location 0/RSP0/CPU0
Router(config-cnbng-nal-local)#ipoe fsol-flow-control 70
Router(config-cnbng-nal-local)#commit
```

  Similarly, for PPPoE packets, use:

```
Router(config-cnbng-nal-local)#pppoe fsol-flow-control 60
```

- **UP notification events flow control:**
  - **UP delete notification flow control**:

The UP delete notification flow control limit ranges from 20 to 400 packets for each second, the default being 100.

```
Router(config-cnbng-nal-local)#up-cp-notification flow-control 70
```

- **UP statistics report flow control**

  The UP statistics report flow control limit ranges from 20 to 500 packets for each second, the default being 150.

```
Router(config-cnbng-nal-local)#up-cp-stats flow-control 70
```

Running Configuration

This is the running configuration on cnBNG UP that includes the basic UP configuration as well:

```
cnbng-nal location 0/RSP0/CPU0
 hostidentifier CNBNG-UP2
 up-server ipv4 192.0.2.1 vrf default
 cp-server primary ipv4 198.51.100.1
 auto-loopback vrf default
  interface Loopback0
   primary-address 1.0.0.1
  !
 !
disable-secondary-address-notification
cp-association retry-count 10
ipoe fsol-flow-control 70
pppoe fsol-flow-control 60
up-cp-notification flow-control 70
up-cp-stats flow-control 70
max-create-in-progress 600
secondary-address-update enable
!
```

Verification

Use the following **show** command to see the respective packet counters and to check the packet drops. Check the **V4 DHCP FSOL drop flow ctrl** and **V6 DHCP FSOL drop flow ctrl** parameters in this output.

```
Router#show cnbng-nal counters type all
Thu Feb  3 11:13:49.767 UTC

Location: 0/RSP0/CPU0
.
.
.
Packet Counters
------------------

.
.
.
Counter name                                Value
=============                               =====
V4 DHCP FSOL drop flow ctrl                 9490
V6 DHCP FSOL drop flow ctrl                 241350
.
```

.
.