IP Overlapping Address Pools

The IP Overlapping Address Pools feature improves flexibility in assigning IP addresses dynamically. This feature allows you to configure overlapping IP address pool groups to create different address spaces and concurrently use the same IP addresses in different address spaces.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

Restrictions for IP Overlapping Address Pools

The Cisco IOS XE software checks for duplicate addresses on a per-group basis. The check for duplicate addresses means that you can configure pools in multiple groups that could have possible duplicate addresses. The IP Overlapping Address Pools feature should be used only in cases where overlapping IP address pools make sense, such as Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environments where multiple IP address spaces are supported.

Information About IP Overlapping Address Pools

Benefits

The IP Overlapping Address Pools gives greater flexibility in assigning IP addresses dynamically. It allows you to configure overlapping IP address pool groups to create different address spaces and concurrently use the same IP addresses in different address spaces.

How IP Address Groups Work

IP Control Protocol (IPCP) IP pool processing implements all IP addresses as belonging to a single IP address space, and a given IP address should not be assigned multiple times. IP developments such as virtual private dialup network (VPDN) and Network Address Translation (NAT) implement the concept of multiple IP address spaces where it can be meaningful to reuse IP addresses, although such usage must ensure that these duplicate address are not placed in the same IP address space. An IP address group to support multiple IP address spaces and still allow the verification of nonoverlapping IP address pools within a pool group. Pool names must be unique within the router. The pool name carries an implicit group identifier because that pool name can be associated only with one group. Pools without an explicit group name are considered members of the base system group and are processed in the same manner as the original IP pool implementation.

Existing configurations are not affected by the new pool feature. The “group” concept is an extension of the existing **ip local pool** command. Processing of pools that are not specified as a member of a group is unchanged from the existing implementation.

How to Configure IP Overlapping Address Pools

Configuring and Verifying a Local Pool Group

Perform this task to configure a local pool group and verify that it exists.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip local pool** {**default** | *poolname*} {*low-ip-address* [*high-ip-address*] [**group** *group-name*] [**cache-size** *size*]}
4. **show ip local pool** [*poolname* | [**group** *group-name*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip local pool** {**default** | *poolname*} {*low-ip-address* [*high-ip-address*] [**group** *group-name*] [**cache-size** *size*]} **Example:** `Router(config)# ip local pool testpool 10.2.2.1 10.2.2.10 group testgroup cache-size 10000`	Configures a group of local IP address pools, gives this group a name, and specifies a cache size.
Step 4	**show ip local pool** [*poolname* | [**group** *group-name*]] **Example:** `Router(config)# show ip local pool group testgroup testpool`	Displays statistics for any defined IP address pools.

Configuration Examples for Configuring IP Overlapping Address Pools

Define Local Address Pooling as the Global Default Mechanism Example

The following example shows how to configure local pooling as the global default mechanism:

```
ip address-pool local
ip local pool default 192.168.15.15 192.168.15.16
```

Configure Multiple Ranges of IP Addresses into One Pool Example

The following example shows how to configure two ranges of IP addresses for one IP address pool:

```
ip local pool default 192.169.10.10 192.169.10.20
ip local pool default 192.168.50.25 192.168.50.50
```

Additional References

The following sections provide references related to configuring IP Overlapping Address Pools.

Related Documents

Related Topic	Document Title
Dial commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Dial Services Command Reference*
IP address pooling	"Configuring Media-Independent PPP and Multilink PPP" chapter of the Cisco IOS XE Dial Technologies Configuration Guide

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 826	*Address Resolution Protocol*
RFC 903	*Reverse Address Resolution Protocol*
RFC 1027	*Proxy Address Resolution Protocol*
RFC 1042	*Standard for the Transmission of IP Datagrams over IEEE 802 Networks*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Glossary

IPCP --IP Control Protocol. Protocol that establishes and configures IP over PPP.

MPLS --Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

NAT --Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as Network Address Translator.

VPDN --virtual private dialup network. Also known as virtual private dial network. A VPDN is a network that extends remote access to a private network using a shared infrastructure. VPDNs use Layer 2 tunnel technologies (L2F, L2TP, and PPTP) to extend the Layer 2 and higher parts of the network connection from a remote user across an ISP network to a private network. VPDNs are a cost-effective method of establishing a long distance, point-to-point connection between remote dial users and a private network. See also VPN.

VPN --Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.

VRF --A VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.