Understanding Multicast Administrative Scoping

* date\_range12-Sep-17
* [info\_outline Platform and Release Support](https://www.juniper.net/documentation/en_US/junos/topics/concept/multicast-administrative-scoping.html)

You use multicast scoping to limit multicast traffic by configuring it to an administratively defined topological region. Multicast scoping controls the propagation of multicast messages—both multicast group join messages that are sent upstream toward a source and data forwarding downstream. Scoping can relieve stress on scarce resources, such as bandwidth, and improve privacy or scaling properties.

IP multicast implementations can achieve some level of scoping by using the time-to-live (TTL) field in the IP header. However, TTL scoping has proven difficult to implement reliably, and the resulting schemes often are complex and difficult to understand.

Administratively scoped IP multicast provides clearer and simpler semantics for multicast scoping. Packets addressed to administratively scoped multicast addresses do not cross configured administrative boundaries. Administratively scoped multicast addresses are locally assigned, and hence are not required to be unique across administrative boundaries.

The administratively scoped IP version 4 (IPv4) multicast address space is the range from 239.0.0.0 through 239.255.255.255.

The structure of the IPv4 administratively scoped multicast space is based loosely on the IP version 6 (IPv6) addressing architecture described in RFC 1884, *IP Version 6 Addressing Architecture*.

There are two well-known scopes:

* IPv4 local scope—This scope comprises addresses in the range 239.255.0.0/16. The local scope is the minimal enclosing scope and is not further divisible. Although the exact extent of a local scope is site-dependent, locally scoped regions must not span any other scope boundary and must be contained completely within or be equal to any larger scope. If scope regions overlap in an area, the area of overlap must be within the local scope.
* IPv4 organization local scope—This scope comprises 239.192.0.0/14. It is the space from which an organization allocates subranges when defining scopes for private use.

The ranges 239.0.0.0/10, 239.64.0.0/10, and 239.128.0.0/10 are unassigned and available for expansion of this space.

Two other scope classes already exist in IPv4 multicast space: the statically assigned link-local scope, which is 224.0.0.0/24, and the static global scope allocations, which contain various addresses.

All scoping is inherently bidirectional in the sense that join messages and data forwarding are controlled in both directions on the scoped interface.

You can configure multicast scoping either by creating a named scope associated with a set of routing device interfaces and an address range, or by referencing a scope policy that specifies the interfaces and configures the address range as a series of filters. You cannot combine the two methods (the commit operation fails for a configuration that includes both). The methods differ somewhat in their requirements and result in different output from the show multicast scopecommand. For details and configuration instructions, see and .

Routing loops must be avoided in IP multicast networks. Because multicast routers must replicate packets for each downstream branch, not only do looping packets not arrive at a destination, but each pass around the loop multiplies the number of looping packets, eventually overwhelming the network.

Scoping limits the routers and interfaces that can be used to forward a multicast packet. Scoping can use the TTL field in the IP packet header, but TTL scoping depends on the administrator having a thorough knowledge of the network topology. This topology can change as links fail and are restored, making TTL scoping a poor solution for multicast.

Multicast scoping is administrative in the sense that a range of multicast addresses is reserved for scoping purposes, as described in RFC 2365. Routers at the boundary must be able to filter multicast packets and make sure that the packets do not stray beyond the established limit.

Administrative scoping is much better than TTL scoping, but in many cases the dropping of administratively scoped packets is still determined by the network administrator. For example, the multicast address range 239/8 is defined in RFC 2365 as administratively scoped, and packets using this range are not to be forwarded beyond a network “boundary,” usually a routing domain. But only the network administrator knows where the border routers are and can implement the scoping correctly.

Multicast groups used by unicast routing protocols, such as 224.0.0.5 for all OSPF routers, are administratively scoped for that LAN only. This scoping allows the same multicast address to be used without conflict on every LAN running OSPF.

The scope field indicates the scope of the IPv6 internetwork for which the multicast traffic is intended. The size of this field is 4 bits. In addition to information provided by multicast routing protocols, routers use multicast scope to determine whether multicast traffic can be forwarded. For multicast addresses there are 14 possible scopes (some are still unassigned), ranging from interface-local to global (including both link-local and site-local).

The following table lists the defined values for the scope field:

| **Value** | **Scope** |
| --- | --- |
| 0 | Reserved |
| 1 | Interface-local scope (same node) |
| 2 | Link-local scope (same link) |
| 3 | Subnet-local scope |
| 4 | Admin-local scope |
| 5 | Site-local scope (same site) |
| 8 | Organization-local scope |
| E | Global scope |
| F | Reserved |
| All other scope field values are currently undefined. | |
| *Table 1. Multicast scope field values* | |

For example, traffic with the multicast address of FF02::2 has a link-local scope. An IPv6 router never forwards this type of traffic beyond the local link.

**Interface-local**

The interface-local scope spans a single interface only. A multicast address of interface-local scope is useful only for loopback delivery of multicasts within a node, for example, as a form of interprocess communication within a computer. Unlike the unicast loopback address, interface-local multicast addresses may be joined on any interface.

**Link-local**

Link-local addresses are used by nodes when communicating with neighboring nodes on the same link. The scope of the link-local address is the local link.

**Subnet-local**

Subnet-local scope is given a different and larger value than link-local to enable possible support for subnets that span multiple links.

**Admin-local**

Admin-local scope is the smallest scope that must be administratively configured, that is, not automatically derived from physical connectivity or other, non-multicast-related configuration.

**Site-local**

The scope of a site-local address is the site or organization internetwork. Addresses must remain within their scope. A router must not forward packets outside of its scope.

**Organization-local**

This scope is intended to span multiple sites belonging to a single organization.

**Global**

Global scope is used for uniquely identifying interfaces anywhere in the Internet.

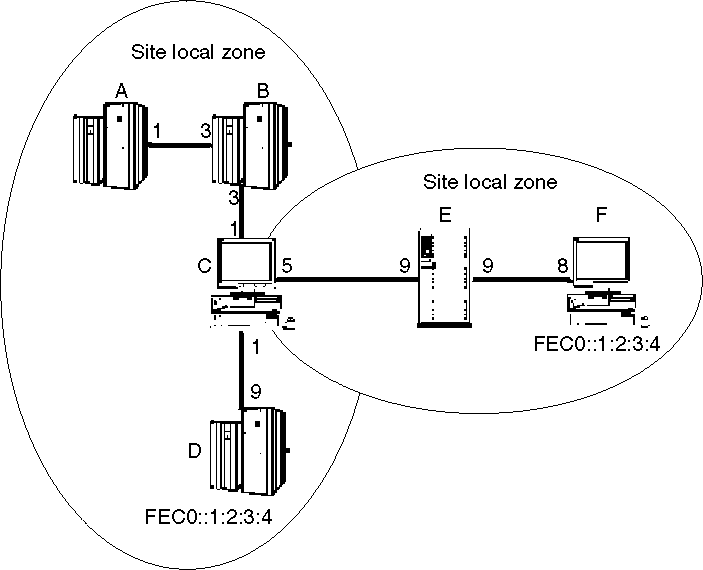
Site-local addresses have the following format:

| **10 bits** | **38 bits** | **16 bits** | **64 bits** |
| --- | --- | --- | --- |
| 1111111011 | 0 | subnet ID | interface ID |
| *Table 1. Site-local address format* | | | |

Site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix. A site-local address cannot be reached from another site. A site-local address is not automatically assigned to a node. It must be assigned using automatic or manual configuration.

Routers will not forward any packets with site-local source or destination addresses outside of the site.

Figure 1. Site-local scope zones



Nodes connected to the same site-local scope zone may communicate with each other using site-local addresses. However, nodes which are not connected to the same site-local scope zone may not communicate using site-local addresses but must instead use global addresses.

[Figure 1](https://www.ibm.com/support/knowledgecenter/SSB27U_7.1.0/com.ibm.zvm.v710.kijl0/kijl035.htm?view=kc#kijl0-gen34__kijl0i02) depicts two site-local scope zones. In this configuration, node A can communicate with node D using site-local addresses since they are both within the same site-local scope zone. However, node A cannot communicate with node F using site-local addresses because the two nodes are not connected to the same site-local scope zone. Instead, node A must use global addresses when communicating with node F. Since node C is connected to both site-local scope zones, it may use the appropriate site-local address when communicating with both node A and node F.

The TCP/IP for z/VM server supports connecting to a single site-local scope zone and cannot be connected to two or more site-local scope zones at the same time. For example, the TCP/IP for z/VM server could be either node A or node F in [Figure 1](https://www.ibm.com/support/knowledgecenter/SSB27U_7.1.0/com.ibm.zvm.v710.kijl0/kijl035.htm?view=kc#kijl0-gen34__kijl0i02), as both are connected to only a single site-local scope zone, but could not be node C, as node C is connected to two site-local scope zones.