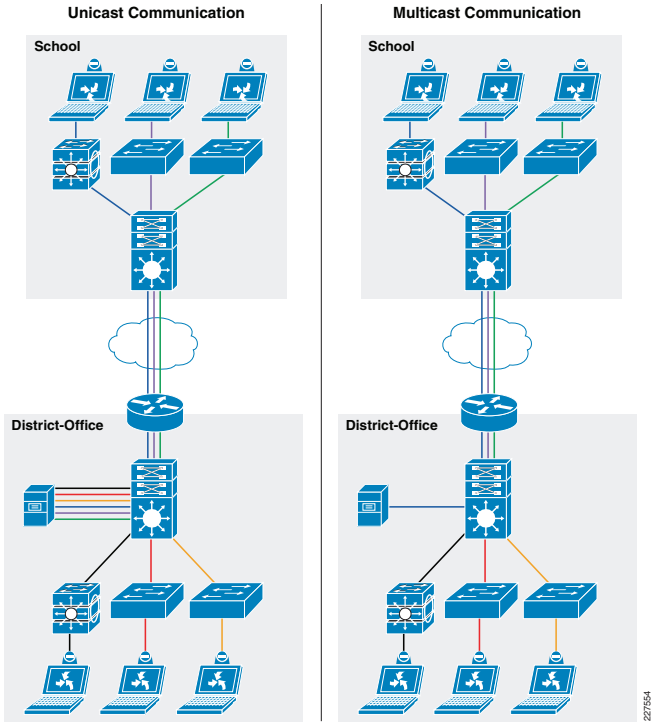
This document describes the Schools Service Ready Architecture Network Multicast Design,

Communications in a IP network can be:

- Unicast—One source sends a message to one destination.
- Broadcast—One source sends a message to all destinations
- Multicast—One source sends a message to a subset of destinations

IP multicast allows a source to transmit a message as a group transmission to a subset of hosts on the network. Many collaboration applications, such as video conferencing, distance learning, software distribution, utilize multicast techniques. IP multicast improves network bandwidth utilization, by reducing un necessary duplicate traffic. Multicast improves efficiency by reducing data processing on the source server, and sending a single flow into the network. Multicast packets are replicated in the network where paths diverge, by Protocol Independent Multicast (PIM) enabled routers, and other supporting multicast protocols. See Figure 1.

Figure 1 Unicast versus Multicast Communication in School Network



Multicast IP Addressing

The Internet Assigned Numbers Authority (IANA) controls the assignment of IP multicast addresses. A range of class D address space is assigned for IP multicast applications. All multicast group addresses fall in the range of 224.0.0.0 through 239.255.255.255. In IP multicast packets, the destination IP address is in the multicast group range, while the source IP address is always in the unicast address range. The multicast IP address space is further divided into several pools for well-known multicast network protocols, and inter-domain multicast communications as shown in Table 1.

Table 1 Multicast Address Range Assignments

Application	Address Range
Reserved – Link Local Network Protocols	224.0.0.0/24
Globally Scope – Group communication between organization and Internet	224.0.1.0 – 238.255.255.255
Source Specific Multicast (SSM) – PIM extension for one-to-many unidirectional multicast communication	232.0.0.0/8
GLOP – Inter-domain Multicast group assignment with reserved global Autonomous System (AS)	233.0.0.0/8
Limited Scope – Administratively scope address that remains constrained within local organization or AS. Commonly deployed in enterprise, education and other organization.	239.0.0.0/8

For the Schools SRA network design, the multicast IP addresses must be selected from the Limited Scope pool (239.0.0.0/8).

Multicast Routing Design

Each device between a multicast source and receiver must enable dynamic multicast. The technique for creating a multicast forwarding table is different than unicast routing and switching techniques. Multicast requires 'Multicast Routing Protocol' and 'Dynamic Group Membership' to enable communication.

Multicast Routing Protocol

IP multicast delivers source traffic to multiple receivers using the least amount of network resources, without placing additional burden on the source or the receivers. Multicast packet replication in the network is performed by Cisco routers and switches enabled with Protocol Independent Multicast (PIM) and other multicast routing protocols.

The network must build a packet distribution tree that specifies a unique forwarding path between the source subnet and each multicast group members subnet. A primary goal for the tree is to ensure that only one copy of each packet is forwarded on each branch of the tree. The two basic types of multicast distribution trees are source trees and shared trees:

- Source trees—The simplest form of a multicast distribution tree is a source tree, with the source at the root and the receivers at the branches. Because this tree uses the shortest path through the network, it is also referred to as a shortest path tree (SPT).
- Shared trees—A shared tree uses a single common root placed at a chosen point in the network. This shared root is called a Rendezvous Point (RP).

PIM protocol has two modes which support both types of multicast distribution trees:

- Dense Mode—This mode assumes that most routers in the network will distribute multicast traffic to each multicast group. PIM-DM builds distribution trees by initially flooding the entire network and then pruning back the small number of paths without receivers.
- Sparse Mode—This mode assumes that relatively few routers in the network will be involved in each multicast group. The hosts belonging to the group are usually widely dispersed, as would be the case for most multicast over the WAN. PIM-SM begins with an empty distribution tree and adds branches only as the result of explicit IGMP requests to join.

It is recommended to deploy multicast in PIM-SM in the Schools SRA. All the recommended platforms in this design support PIM-SM mode on physical or logical (SVI and EtherChannel) interfaces.

Dynamic Group Membership

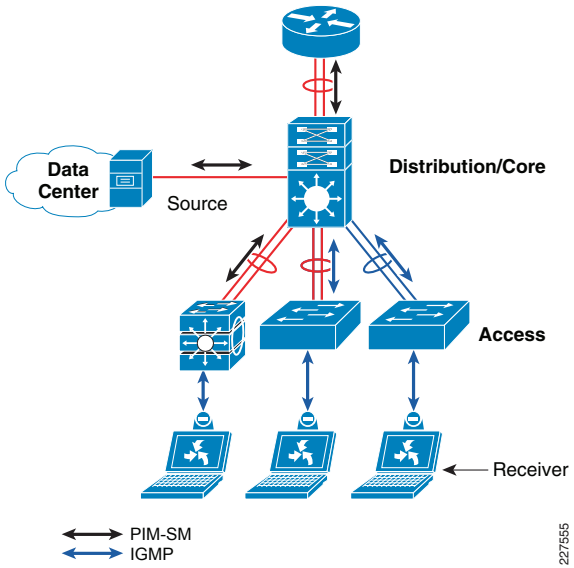
Multicast receiver registration and deletion is done via Internet Group Management Protocol (IGMP) signaling. IGMP operates between a multicast receiver in the access-layer and a collapsed core router at the distribution layer in the district office or the school site.

In a multi-layer design, the Layer-3 boundary is at the distribution switch. Multi-layer access-switches do not run PIM, and therefor flood the traffic on all ports. This multi-layer access-switch limitation is solved by using IGMP snooping feature, which is enabled by default. Best practice is to not disable IGMP snooping feature.

In a routed-access network design, the Layer-3 boundary is at the access-layer and IGMP communication is between receiver and access-switch. Along with unicast routing protocol, PIM-SM must be enabled on the Layer 3 access-switch to communicate with RP in the network.

Figure 2 demonstrates multicast source and receiver registration procedure and how shared-tree is dynamically developed for multicast data delivery.

Figure 2



Deploying PIM-SM

Multicast data delivery in the network is “connection-oriented”. Multicast communication does not get triggered by data, instead it requires a registration procedure to detect the source and receiver and develop the path. Multicast registration procedure is handled by PIM protocol in the network, and when PIM is deployed in Sparse-Mode registration process is handled by RP.

PIM-SM Rendezvous Point

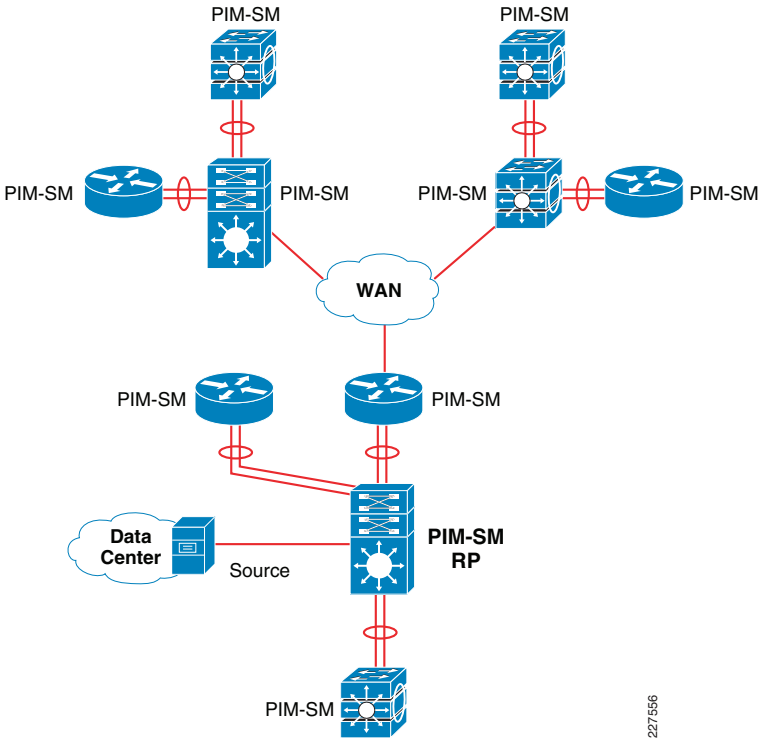
PIM-SM distributes information about active sources by forwarding data packets on the shared tree. Because PIM-SM uses shared trees initially, it requires the use of a RP. It is recommended to deploy the RP close to the multicast source (collapsed core-distribution router in the district office is a good choice). Multicast sources centrally deployed in district office will register themselves with the RP and then data is forwarded down the shared tree to the receivers that could be located anywhere in the network.

PIM-SM supports RP deployment in the following three different modes in the network:

- Static—As the name implies, RP must be statically identified and configured on each PIM router in the network. RP load-balancing and redundancy can be achieved using Anycast RP.
- Auto-RP—Dynamic method to discover and announce RP in the network. Auto-RP implementation is beneficial when there are multiple RPs and groups that often change in the network. To prevent network reconfiguration during change, RP mapping agent router must be designated in the network to receive RP group announcements and arbitrate conflicts. This capability is part of PIM version 1 specification.
- BootStrap Router (BSR)—Performs same task as Auto-RP but different mechanism. This capability is pare of PIM version 2 specification. Auto-RP and BSR cannot coexist or interoperate in the same network.

In a small to mid-size multicast network, static RP configuration is best overall, due primarily to the amount of administrative overhead that Auto-RP or BSR introduce. Static RP implementation offers same RP redundancy and load sharing and a simple ACL can be applied to deploy RP without compromising multicast network security. See Figure 3.

Figure 3 PIM-SM network design in school network infrastructure



Following is an example configuration to deploy PIM-SM RP in the district office. Similar static PIM-SM configuration must be enabled on each Layer-3 PIM router or an access-switch in the school sites:

Distribution - RP

```
cr24-4507-DO(config)#interface Loopback1
cr24-4507-DO(config-if)# description RP
cr24-4507-DO(config-if)# ip address 10.125.100.100 255.255.255.255
cr24-4507-DO(config)#ip multicast-routing
cr24-4507-DO(config)#ip pim rp-address 10.125.100.100
```

Layer 3 Access

```
cr24-3560r-DO(config)#ip multicast-routing distributed
cr24-3560r-DO(config)#ip pim rp-address 10.125.100.100
```

School Core

```
cr36-3750s-ss100(config)#ip multicast-routing distributed
cr36-3750s-ss100(config)#ip pim rp-address 10.125.100.100
```

Upon successful PIM-SM RP implementation throughout the school network, PIM-SM must be enabled on Layer-3 edge and core network-facing ports. The following sample configuration provides a simple PIM-SM implementation guideline to be implemented on every intermediate Layer-3 systems between receiver and source:

Distribution - RP

```
! District Office - Access Network
cr24-4507-DO(config)#interface range Vlan101 - 140
cr24-4507-DO(config-if-range)# ip pim sparse-mode

! District Office - Data Center Network
cr24-4507-DO(config)#interface range Vlan141 - 150
cr24-4507-DO(config-if-range)# ip pim sparse-mode

! Layer 3 Core and Routed-Access Port-Channel
cr24-4507-DO(config)#interface range Port-channel 1, Port-channel 13,
Port-channel 15
cr24-4507-DO(config-if-range)# ip pim sparse-mode


cr24-4507-DO#show ip pim interface
Address          Interface Ver/   Nbr    Query  DR     DR
                                         Mode   Count  Intvl  Prior
10.125.32.4      Port-channel1v2/S   1      30     1    10.125.32.4
<omitted>
10.125.1.1       Vlan101         v2/S 0      30     1      10.125.1.1

cr24-4507-DO#show ip mroute sparse
(*, 239.192.51.8), 02:33:37/00:03:12, RP 10.125.100.100, flags: SJC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan111, Forward/Sparse, 02:04:33/00:02:44, H
    Vlan101, Forward/Sparse, 02:04:59/00:02:58, H
    Port-channel15, Forward/Sparse, 02:04:59/00:02:47, H
    Vlan131, Forward/Sparse, 02:04:59/00:02:32, H
    Port-channel13, Forward/Sparse, 02:04:59/00:03:12, H
    Vlan121, Forward/Sparse, 02:04:59/00:02:14, H
    Vlan146, Forward/Sparse, 02:21:26/00:02:01, H
```

Layer 3 Access

```
! District Office - Layer 3 Access Network
cr24-3560r-DO(config)#interface range Vlan11 - 20
cr24-3560r-DO(config-if-range)# ip pim sparse-mode

! Routed-Access Port-Channel
cr24-4507-DO(config)#interface Port-channel 1
cr24-4507-DO(config-if)# ip pim sparse-mode

cr24-3560r-DO#show ip pim interface
Address          Interface Ver/   Nbr    Query  DR      DR
                                  Mode   Count  Intvl   Prior
10.125.32.1Port-channel1v2/S   1      30     1       10.125.32.0
10.125.11.1      Vlan11v2/S   0      30     1       10.125.11.1
```

Implementing IGMP

By default the Layer-2 access-switch will dynamically detect IGMP hosts and multicast-capable Layer-3 routers in the network. The IGMP snooping and multicast router detection functions on a per VLAN basis, and is globally enabled by default for all the VLANs. The IGMP configuration can be validated using the show command on the Layer-2 access-switch:

```
cr24-2960-DO#show ip igmp snooping
Global IGMP Snooping configuration:
-----------------------------------------------
IGMP snooping               : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

cr24-2960-DO#show ip igmp snooping mrouter
Vlan    ports
------    ------
 101    Po1(dynamic)
 102    Po1(dynamic)

cr24-2960-DO#show ip igmp snooping group
Vlan      GroupType        Version     Port List
------------------------------------------------------------------------
101       239.192.51.1igmp        v2     Fa0/1, Po1
101       239.192.51.2igmp        v2     Fa0/2, Po1
```

Multicast routing function changes when the access-switch is deployed in routed-access mode. PIM operation is performed at the access layer; therefore, multicast router detection process is eliminated. The following output from a Layer-3 switch verifies that the local multicast ports are in router mode, and provide a snooped Layer-2 uplink port-channel which is connected to the collapsed core router, for multicast routing:

```
cr24-3560r-DO#show ip igmp snooping mrouter
Vlan    ports
------    ------
  11    Router
  12    Router

cr24-3560r-DO#show ip igmp membership | inc Channel|Vl
 Channel/Group                  Reporter        Uptime       Exp.Flags
Interface
 *,239.192.51.8                 10.125.11.2000:17:52  02:45 2A     Vl11
 *,239.192.51.9                 10.125.11.13100:17:52  02:43 2A     Vl12
```

Multicast Security—Preventing Rogue Source

This section provides basic multicast security configuration guidelines to prevent an unauthorized host in the network from acting like a rogue source in the network and sending multicast traffic.

In a PIM-SM network, an unwanted traffic source can be controlled with the pim accept-register command. When the source traffic hits the first-hop router, the first-hop router (DR) creates (S,G) state and sends a PIM Source Register message to the RP. If the source is not listed in the accept-register filter list (configured on the RP), then the RP rejects the Register and sends back an immediate Register-Stop message to the DR. The drawback with this method of source-filtering is that the pim accept-register command on the RP, PIM-SM (S,G) state is still created on the source's first-hop router. This can result in traffic reaching receivers local to the source and located between the source and the RP. Furthermore, the pim accept-register command works on the control plane of the RP, which could be used to overload the RP with "fake" register messages, and possibly cause a DoS condition.

Best practice is to apply the pim accept-register command on the RP in addition to other edge-filtering methods, such as simple data plane ACLs on all DRs and on all ingress points into the network. While ingress ACLs on the DR are sufficient in a perfectly configured and operated network, best practice includes configuring the pim accept-register command on the RP in the district office as a secondary security mechanism in case of misconfiguration on the edge routers.

Following is the sample configuration with a simple ACL which has been applied to the RP to filter only on the source address. It is also possible to filter the source and the group with the use of an extended ACL on the RP:

Distribution-RP

```
cr24-4507-DO(config)#ip access-list extended PERMIT-SOURCES
cr24-4507-DO(config-ext-nacl)# permit ip 10.125.31.80 0.0.0.15
239.192.0.0 0.0.255.255

cr24-4507-DO(config)#ip pim accept-register list PERMIT-SOURCES
```

Multicast Security—Preventing Rogue RP

Any router can be misconfigured or maliciously advertise itself as a multicast RP in the network. with the valid multicast group address. With a static RP configuration, each PIM-enabled router in the network can be configured to use the static RP for the multicast source and ignore any Auto-RP or BSR multicast router announcement.

Following is the sample configuration that must be applied to each PIM-enabled router in the district office and school sites, to accept PIM announcements only from the static RP and ignore dynamic multicast group announcement from any other RP:

Distribution-RP

```
cr24-4507-DO(config)#ip access-list standard Allowed_MCAST_Groups
cr24-4507-DO(config-std-nacl)# permit 224.0.1.39
cr24-4507-DO(config-std-nacl)# permit 224.0.1.40
cr24-4507-DO(config-std-nacl)# permit 239.192.0.0 0.0.255.255

cr24-4507-DO(config)#ip pim rp-address 10.125.100.100
Allowed_MCAST_Groups override

cr24-4507-DO#show ip pim rp mapping
PIM Group-to-RP Mappings
Acl: Allowed_MCAST_Groups, Static-Override
    RP: 10.125.100.100 (?)
```