Network Policies Help

# **VRF Policies**

* **Tags** [annotations] – A search keyword or term that is assigned to the VRF. Tags allow you to group multiple objects by descriptive names. You can assign the same tag name to multiple objects and you can assign one or more tag names to a single object.
* **Global Alias** [name\_alias] – A changeable name for a given object. While the name of an object, once created, cannot be changed, the Alias is a field that can be changed.
* **Policy Control Enforcement Preference** [pc\_enf\_pref] – The preferred policy control. The policy enforcement can be:
  + **Enforced**—Security rules (contracts) will be enforced.
  + **Unenforced**—Security rules (contracts) will not be enforced.

The default is ***Enforced.***

* **Policy Control Enforcement Direction** [pc\_enf\_dir] – Defines the policy enforcement direction coming to or from a Layer 3 Outside connection (L3Out). The direction can be:
  + **Ingress**—Policy is enforced on ingress traffic.
  + **Egress**—Policy is enforced on egress traffic.

The default is ***Ingress***.

* **BD Enforcement Status** [bd\_enforce] – Set the BD Enforcement Status to “yes” to enable this condition: Only allow endpoints to ping their bridge domain gateways. Ping from hosts on different bridge domains cannot ping other gateways.

You can then create a global exception list of IP addresses which can ping any subnet gateway.

The default is ***no***.

* **Enforcement Type** [enf\_type]:
  + **Contract –** Apply consumer/provider filtering at the EPG level. Use for macro/micro access control.
  + **Preferred-group –** Preferred group allows you to whitelist traffic between all EPG’s that are members of the preferred group, i.e., have preferred group enabled. This includes external EPG’s. This must be enabled at the VRF level and then applied to each individual EPG. EPGs that do not have preferred group enabled will not be allowed to communicate to preferred group members without a contract.
  + **vzAny** **–** Apply consumer/provider filtering at the VRF level.
* **BGP Timers** [bgpCtxPol] – Assign the BGP timers policy associated with this VRF. Anything other than default will require the Distinguish Name. “bgpCtxPol” is the API Class Name.   
  Example: “uni/tn-common/bgpCtxP-default”.
* **BGP Context Per Address Family Timers** [bgpCtxAfPol] – Assign the BGP Timers policy for the VRF to the IPv4 and IPv6 Address Families. Anything other than default will require the Distinguish Name. “bgpCtxAfPol” is the API Class Name.   
  Example: “uni/tn-common/bgpCtxAfP-default”.
* **OSPF Timers** [ospfCtxPol] – Assign the OSPF timers policy associated with this VRF. Anything other than default will require the Distinguish Name. “ospfCtxPol” is the API Class Name.  
  Example: “uni/tn-common/ospfCtxP-default”.
* **OSPF Context Per Address Family** [ospfCtxAfPol] – Assign the OSPF Timers policy for the VRF to the IPv4 and IPv6 Address Families. Anything other than default will require the Distinguish Name. “ospfCtxPol” is the API Class Name.  
  Example: “uni/tn-common/ospfCtxP-default”.
* **Endpoint Retention Policy Association** [fvEpRetPol] – Use "default" for "uni/tn-common/epRPol-default". If not default, use the Distinguished Name as shown, for the policy you wish to use. Only Modify if you have defined an alternate policy. “fvEpRetPol” is the API Class Name.
* **Monitoring Policy** **Association** [monEPGPol] –Use "default" for "uni/tn-common/monepg-default". If not default, use the Distinguished Name as shown, for the policy you wish to use. Only modify if you have defined an alternate policy. The policies created by this script only created/modified default policies under the Fabric/Access policies. It would be more advisable if you want to make changes to the policy that are fabric wide make the minor changes to the default policy, rather than using alternate policies. “monEPGPol” is the API Class Name.
* **EIGRP Context Per Address Family Timers** [eigrpCtxAfPol] – Assign the OSPF Timers policy for the VRF to the IPv4 and IPv6 Address Families. Anything other than default will require the Distinguish Name. “eigrpCtxAfPol” is the API Class Name.   
  Example: “uni/tn-common/ospfCtxP-default”.
* **Transit Route Tag Policy** [l3extRouteTagPol] – blah
* **IP Data-plane Learning** [dp\_learning] – Defines if IP addresses are learned through dataplane packets for the VRF.

When disabled, IP addresses are not learned from the dataplane. Local and remote MAC addresses are still learned, but local IP addresses are not. Remote IP addresses are not learned from unicast packets but are learned from multicast packets.

Note: Regardless if this parameter is enabled or disabled, local IP addresses can still be learned from ARP, GARP, and ND.   
The default is ***Enabled***.

* **Known Multicast Allow** [knw\_mcast] – blah
* **I Don’t Know what this is** [l3extVrfValidationPol] – Use "default" for "uni/tn-common/vrfvalidationpol-default". If you wish to use something other than default, use the Distinguished Name as is shown in the quotes. Only Modify if you have defined an alternate policy. “l3extVrfValidationPol” is the API Class Name.

# **BD Policies**

* **Tags** [annotations] – A search keyword or term that is assigned to the VRF. Tags allow you to group multiple objects by descriptive names. You can assign the same tag name to multiple objects and you can assign one or more tag names to a single object.
* **Global Alias** [name\_alias] – A changeable name for a given object. While the name of an object, once created, cannot be changed, the Alias is a field that can be changed.
* **DHCP Relay Policy Association** [dhcpRelayP] – A changeable
* **Bridge Domain Type** [bd\_type] – Specifies whether this bridge domain supports Fibre Channel Over Ethernet (FCoE) communication traffic or regular Ethernet communication traffic. The options are:
  + **fc**—Supports FCoE communication over the ACI fabric.
  + **regular**—Supports normal Ethernet communications over the ACI fabric.

Note: The FCoE protocol is typically used to support communication between SAN storage devices running on a Fibre Channel (FC) network and host applications running on a non-FC network.

The default is ***regular.***

* **Advertise Host Routes** [host\_routing] – Enabling Host Based Routing on the bridge domain, individual host-routes (/32 prefixes) are advertised from the border leaf switches.

Border leaf switches along with the subnet advertise the individual endpoint (EP) prefixes. The route information is advertised only if the host is connected to the local POD. If the EP is moved away from the local POD or once the EP is removed from EP database, the route advertise is then withdrawn.

The default is ***no***.

* **L2 Unknown Unicast** [unk\_mac] – By default, unicast traffic is flooded to all Layer 2 ports. If enabled, unicast traffic flooding is blocked at a specific port, only permitting egress traffic with MAC addresses that are known to exist on the port. The method can be:
  + **Flood**
  + **Hardware** **Proxy**

When the BD has L2 Unknown Unicast set to Flood, if an endpoint is deleted the system deletes it from both the local leaf switches as well as the remote leaf switches where the BD is deployed, by selecting Clear Remote MAC Entries. Without this feature, the remote leaf continues to have this endpoint learned until the timer expires.

**CAUTION**: **Modifying the L2 Unknown Unicast setting causes traffic to bounce (go down and up) on interfaces to devices attached to EPGs associated with this bridge domain.**

The default is ***Hardware Proxy***. Always change to flood if the BD extends outside ACI.

* **L3 Unknown Multicast Flooding** [unk\_mcast] – The node forwarding parameter for Layer 3 unknown Multicast destinations. The value can be:
  + **Flood**—Send the data to the front panel ports if a router port exists on any bridge domain or send the data to the fabric if the data is in transit.
  + **Optimize** **Flood**—Send the data only to router ports in the fabric.

The default is ***Flood***.

* **IPv6 L3 Unknown Multicast** [v6unk\_mcast] – The node forwarding parameter for Layer 3 unknown IPv6 Multicast destinations. The value can be:
  + **Flood**—Send the data to the front panel ports if a router port exists on any bridge domain or send the data to the fabric if the data is in transit.
  + **Optimize** **Flood**—Send the data only to M-router ports in the fabric.

The default is ***Flood***.

* **Multi Destination Flooding** [multi\_dst] – The multiple destination forwarding method for L2 Multicast, Broadcast, and Link Layer traffic types. The method can be:
  + **Flood in BD**—Sends the data to all ports on the same bridge domain.
  + **Drop**—Drops Packet. Never sends the data to any other ports.
  + **Flood in Encapsulation**—Sends the data to the ports on the same VLAN within the bridge domain regardless of the EPG, with the exception that data for the following protocols is flooded to the entire bridge domain:
    - ARP/GARP
    - BGP
    - EIGRP
    - IGMP
    - IS-IS
    - OSPF/OSPFv6
    - ND
    - PIM

The default is ***Flood in BD***.

* **PIM** [mcast\_allow] – Enables the Protocol Independent Multicast (PIM) protocol.  
  The default is ***no***.
* **PIMv6** [ipv6\_mcast] – Enables the Protocol Independent Multicast (PIM) IPv6 protocol.  
  The default is ***no***.
* **IGMP Snooping Policy Association** [igmpSnoopPol] – A changeable
* **ARP Flooding** [arp\_flood] – Enables ARP flooding, so that the Layer 2 broadcast domain maps IP addresses to the MAC addresses. If flooding is disabled, unicast routing will be performed on the target IP address.  
  The default is ***no***. If the BD extends outside of ACI, always set to yes.
* **Limit Local IP Learning to BD/EPG Subnet(s)** [limit\_learn] – Limits IP address learning to the bridge domain subnets only. Every bridge domain can have multiple subnets associated with it. By default, all IP addresses are learned.

The default is ***no***, but we recommend it to be yes.

* **Endpoint Retention Policy Association** [fvEpRetPol] – Provides the parameters for the lifecycle of the endpoint group in the bridge domain. This will assign the policy to the BD. Assign using the Distinguished Name. Example: “uni/tn-common/epRPol-default”.
* **IGMP Snooping Policy Association** [igmpSnoopPol] – IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers and filter multicasts links that do not need them, thus controlling which ports receive specific multicast traffic. This option will assign the IGMP Snooping policy to the bridge domain. Assign using the Distinguished Name. Example: “uni/tn-common/snPol-default”.
* **MLD Snoop Policy Association** [mldSnoopPol] – The Multicast Listener Discovery (MLD) Snooping policy enables the efficient distribution of IPv6 multicast traffic between hosts and routers. It is a Layer 2 feature that restricts IPv6 multicast traffic within a bridge domain to a subset of ports that have transmitted or received MLD queries or reports. Assign using the Distinguished Name. Example: “uni/tn-common/mldsnoopPol-default”.
* **Unicast Routing** [unicast\_route] – enable or disable unicast routing on the Bridge Domain.   
  The default is ***yes***. We recommend disabling if you have not configured a subnet on the BD.
* **Custom MAC Address** [mac] – The MAC address of the bridge domain (BD) or switched virtual interface (SVI). By default, a BD takes the fabric wide default MAC address of 00:22:BD:F8:19:FF. Configure this property to override the default address.
* **EP Move Detection Mode** [ep\_move] – When the GARP based detection option is enabled, Cisco ACI will trigger an endpoint move based on GARP packets if the move occurs on the same interface and same EPG.

The Default is ***no, but it is a best practice to set to yes*.**

* **Route Profile Association** [rtctrlProfile] – Assign a Route Control Profile (route-maps with prefix lists or community lists) to the Bridge Domain. Assign using the Distinguished Name. Example: “uni/tn-common/prof-default”. Note that there is no default Route Maps for Route Control. Create one first.
* **ND Policy Association** [ndIfPol] – Assign a Neighbor discovery (ND) Interface policy, that supports IPv6 services for the bridge domain.
* **Link-local IPv6 Address** [ll\_addr] – Link-Local IPv6 address (LLA) for the bridge domain.
* **BD stretched to Remote Sites** [intersight\_l2] – Extend the Bridge Domain between ACI Fabrics.

The Default is ***no*.**

* **Allow BUM traffic on Stretched BD** [intersight\_bum] – When extending the bridge domain between sites this option is to permit broadcast unknown multicast (BUM) traffic between the sites.

The Default is ***no*.**

* **Optimize WAN Bandwidth** [optimize\_wan] – A changeable
* **Monitoring Policy** **Association** [monEPGPol] –Use "default" for "uni/tn-common/monepg-default". If not default, use the full qualification Distinguished Name as shown, for the policy you wish to use. Only modify if you have defined an alternate policy. The policies created by this script only created/modified default policies under the Fabric/Access policies. It would be more advisable if you want to make changes to the policy that are fabric wide make the minor changes to the default policy, rather than using alternate policies. “monEPGPol” is the API Class Name.
* **First Hop Security Policy Association** [fhsBDPol] – The First Hop Security policy name. Assign using the Distinguished Name. Example: “uni/tn-common/bdpol-default”.
* **Netflow Monitor Policies Association** [netflowMonitorPol] – One of the following:
  + **NetFlow IP Filter Type**—The IPv4 or IPv6 filter for this bridge domain.
  + **NetFlow Monitor Policy**—The name of the NetFlow monitor policy.
* **IP Data-plane Learning** [ip\_learning] – Controls whether the remote leaf switch should update the IP-to-VTEP information with the source VTEP of traffic coming from this bridge domain. The options are:
  + **yes**: The default setting.
  + **no**: Change this setting to no, only if the bridge domain is to be associated with policy-based redirect (PBR) enabled endpoint groups.

Note: Use caution when changing the default setting for this field. Setting this option to no can cause suboptimal traffic forwarding for non-PBR scenarios.

The default is ***yes.***

# **Subnets Policies**

* **Tags** [annotations] – A search keyword or term that is assigned to the VRF. Tags allow you to group multiple objects by descriptive names. You can assign the same tag name to multiple objects and you can assign one or more tag names to a single object.
* **Global Alias** [name\_alias] – A changeable name for a given object. While the name of an object, once created, cannot be changed, the Alias is a field that can be changed.
* **Subnet Control** [Ctrl] – The subnet control state. The control can be specific protocols applied to the subnet such as IGMP Snooping. The control can be:
  + **ND RA Prefix** [nd] – Enables Neighbor Discovery on the subnet.
  + **No Default SVI Gateway** [no-default-gateway] – When using Cisco ACI Multi-Site with this APIC fabric domain (site), indicates that the VRF, EPG, or BD using this subnet are mirrored from another site, which has a relationship to this site through a contract. Do not modify or delete the mirrored objects.
  + **Querier IP** [querier] – Enables IGMP Snooping on the subnet.

The default is **“*nd”*.**

* **Make this IP address primary** [preferred] – Indicates if the subnet is the primary IP address for the bridge domain (preferred over the available alternatives).

The default is ***no***.

* **Scope** [scope] – The network visibility of the subnet. The scope can be:
  + **Private to VRF (private)**—The subnet applies only within its tenant.
  + **Advertised Externally (public)**—The subnet can be exported to a routed connection.
  + **Shared between VRFs (shared)**—The subnet can be shared with and exported to multiple contexts (VRFs) in the same tenant or across tenants as part of a shared service. An example of a shared service is a routed connection to an EPG present in another context (VRF) in a different tenant. This enables traffic to pass in both directions across contexts (VRFs). An EPG that provides a shared service must have its subnet configured under that EPG (not under a bridge domain), and its scope must be set to advertised externally, and shared between VRFs.

Note: Shared subnets must be unique across the contexts (VRF) involved in the communication. When a subnet under an EPG provides a Layer 3 external network shared service, such a subnet must be globally unique within the entire ACI fabric.

The default is ***Private to VRF*** ***(private)***.

* **Treat as Virtual IP address** [virtual] – An IP address that doesn't correspond to an actual physical network interface, that is shared by multiple devices.

This is typically used for the Common Pervasive Gateway use case. For more information, see Common Pervasive Gateway in Cisco APIC Layer 3 Configuration Guide.

The default is ***no***.

* **Route Profile** [rtctrlProfile]– Assign a Route Control Profile (route-maps with prefix lists or community lists) to the Subnet. Assign using the Distinguished Name. Example: “uni/tn-common/prof-default”. Note that there is no default Route Maps for Route Control. Create one first.

* **ND RA Prefix Policy** [ndPfxPol] – Assign a Neighbor discovery (ND) Interface policy, that supports IPv6 services for the bridge domain. Assign using the Distinguished Name. Example: “uni/tn-common/ndpfxpol-default”. Note that there is no default Route Maps for Route Control. Create one first.

# **Application Profile Policies**

* **Tags** [annotations] – A search keyword or term that is assigned to the VRF. Tags allow you to group multiple objects by descriptive names. You can assign the same tag name to multiple objects and you can assign one or more tag names to a single object.
* **Global Alias** [name\_alias] – A changeable name for a given object. While the name of an object, once created, cannot be changed, the Alias is a field that can be changed.
* **QoS Class** [prio] – A configurable set of system classes that define the traffic priority for the associated EPG. Each system class manages one lane of traffic. The priority class can be:
  + Unspecified
  + Level1—Class 1 Differentiated Services Code Point (DSCP) value.
  + Level2—Class 2 DSCP value.
  + Level3—Class 3 DSCP value.
  + Level4—Class 4 DSCP value.
  + Level5—Class 5 DSCP value.
  + Level6—Class 6 DSCP value.

The default is ***Unspecified***

* **Monitoring Policy** **Association** [monEPGPol] –Use "default" for "uni/tn-common/monepg-default". If not default, use the Distinguished Name as shown, for the policy you wish to use. Only modify if you have defined an alternate policy. The policies created by this script only created/modified default policies under the Fabric/Access policies. It would be more advisable if you want to make changes to the policy that are fabric wide make the minor changes to the default policy, rather than using alternate policies. “monEPGPol” is the API Class Name.

# **EPG Policies**

* **Tags** [annotations] – A search keyword or term that is assigned to the VRF. Tags allow you to group multiple objects by descriptive names. You can assign the same tag name to multiple objects and you can assign one or more tag names to a single object.
* **Global Alias** [name\_alias] – A changeable name for a given object. While the name of an object, once created, cannot be changed, the Alias is a field that can be changed.
* **Physical Domains** – Assign a Physical domain to the EPG. This can be assigned with the Distinguished Name of the physical domain or the resource name if the domain has been created by the script assign the resource value.
  + **DN Example**: (physDomP) “uni/phys-access\_phys”.
  + **Resource Example**: Most often aci\_physical\_domain.{name}. But the policies created by the script are created with a loop so for access\_phys it would be aci\_physical\_domain.default[\"access\_phys\"].
* **VMM Domains** – Assign a Virtual domain to the EPG. This can be assigned with the Distinguished Name of the physical domain or the resource name if the domain has been created by the script assign the resource value.
  + **DN Example**: (vmmDomP) “uni/vmm-{vmware\_domain}”.
  + **Resource Example**: Example aci\_vmm\_domain.{ vmware\_domain}.
* **Consumer Contracts** [cons\_vzBrCP] – Add a consumer contract to the EPG. Assign using the Distinguished Name. Example: “uni/tn-common/brc-default”.
* **Provider Contracts** [prov\_vzBrCP] – Add a provider contract to the EPG. Assign using the Distinguished Name. Example: “uni/tn-common/brc-default”.
* **EPG Contract Master** [Master\_fvEPg] – Assign the EPG that will serve as contract master for this EPG, from which this EPG will inherit contracts (you must have previously created the contract master EPG. Assign using the Distinguished Name. Example: “uni/tn-common/ap-default/epg-default”.
* **Consumed Contract Interface** [vzCPIf] – Configure a contract for which the EPG will be a consumer. Assign using the Distinguished Name. Example: “uni/tn-common/brc-default”.
* **Provider Default** [vzCtrctEPgCont] – unsure?
* **Taboo Contract** [vzTaboo] – Taboo contracts can be used to deny specific traffic that is otherwise allowed by contracts. The traffic to be dropped matches a pattern (such as, any EPG, a specific EPG, or traffic matching a filter). Taboo rules are unidirectional, denying any matching traffic coming toward an EPG that provides the contract. Taboo rules are applied in the hardware before applying the rules of regular contracts. Assign using the Distinguished Name. Example: “uni/tn-common/taboo-default”.
* **Contract Exception Tag** [exception\_tag] – Contracts between EPGs are enhanced to include exceptions to subjects or contracts. This enables a subset of EPGs to be excluded in contract filtering. For example, a provider EPG can communicate with all consumer EPGs except those that match criteria configured in a Subject Exception in the contract governing their communication. Assign a Tag Attribute to the EPG.
* **uSeg EPG** [is\_attr\_based] – Indicates (true or false) whether this EPG is a micro-segmented EPG, defined by micro-segmentation attributes and identical network behavior.

Note: Micro-segmentation associates endpoints from multiple EPGs into a micro-segmented EPG according to virtual machine attributes, IP address, or MAC address. Virtual machine attributes include: VNIC domain name, VM identifier, VM name, hypervisor identifier, VMM domain, datacenter, operating system, or custom attribute.

* **QoS Class** [prio] – A configurable set of system classes that define the traffic priority for the associated EPG. Each system class manages one lane of traffic. The priority class can be:
  + Unspecified
  + Level1—Class 1 Differentiated Services Code Point (DSCP) value.
  + Level2—Class 2 DSCP value.
  + Level3—Class 3 DSCP value.
  + Level4—Class 4 DSCP value.
  + Level5—Class 5 DSCP value.
  + Level6—Class 6 DSCP value.

The default is ***Unspecified***

* **Custom QoS** [qosCustomPol] – Assign an existing custom QoS policy, default, or click Create Custom QoS Policy. The custom class is a user configurable DSCP value. Assign using the Distinguished Name. Example: “uni/tn-common/qoscustom-default”.
* **Data-Plane Policer** [qosDppPol] – The Data Plane Policer supports only ingress direction. It is supported only on switch models with Cloud Scale ASICs (EX|FX|GX) or later models.
* **Intra EPG Isolation**[pc\_enf\_pref] – Provides complete endpoint isolation within individual application tiers. The intra EPG isolation state can be:
  + **Enforced**
  + **Unenforced**

Note: No communication is allowed between endpoints in an EPG that is operating in full isolation mode. Isolated mode EPGs reduce the number of EPG encapsulations required when many clients access a common service but are not allowed to communicate with each other.

The Default is ***Unenforced***.

* **Intra-EPG Contract** [intra\_vzBrCP] – Assign a contract [with subject and filters] to the Intra-EPG policy.
* **Forwarding Control** [fwd\_ctrl] – Intra EPG isolation must be enforced for the forwarding control field to be displayed.

When enabled, the forwarding control allows Address Resolution Protocol (ARP) by proxy.

* + **proxy-arp**—Proxy ARP is the technique in which one host answers ARP requests intended for another machine. Proxy ARP can help machines on a subnet reach remote subnets without the need to configure routing or a default gateway.
* **Preferred Group Member** [pref\_gr\_memb] – If an EPG is marked as a Preferred Group Member, it is put into an internally created contract group where all members of the group can communicate with each other without requiring a contract between them.

The options are:

* + **Exclude**—The EPG is not included in the subgroup.
  + **Include**—The EPG is included in the subgroup.

The default is ***Exclude***.

* **Flood on Encapsulation** [flood] – Specifies whether flooding is enabled for the EPG or not. If flooding is disabled, the value specified in the BD mode is considered.

The Default is ***disabled*.**

* **Label Match Criteria** [match\_t] – The match criteria can be:
  + **All**
  + **AtleastOne**
  + **AtmostOne**
  + **None**—no labeling matching

The default is ***AtleastOne***.

* **Monitoring Policy** [monEPGPol] –Use "default" for "uni/tn-common/monepg-default". If not default, use the Distinguished Name as shown above, for the policy you wish to use. Only modify if you have defined an alternate policy. The policies created by this script only created/modified default policies under the Fabric/Access policies. It would be more advisable if you want to make changes to the policy that are fabric wide make the minor changes to the default policy, rather than using alternate policies. “monEPGPol” is the API Class Name.
* **FHS Trust Control Policy** [fhsTrustCtrlPol] – The First Hop Security Trust Control policy name. Assign using the Distinguished Name. Example: “uni/tn-common/trustctrlpol-default”.
* **shutdown** [shutdown] – This option will disable the EPG if set to yes.
* **Has Multicast Source** [has\_mcast] – A
* **Fabric Node** [fabricNode] – A
* **Fabric Endpoint** [fabricPathEp] – A
* **Don't Know** [vzGraphCont] – A