# Contents

# Sites Help Section

## Sites

- **Site_ID**
- **Site_Name**
- **APIC**
- **BGP_AS**
- **SNMP_Location**
- **Contract_ID**
- **Customer_Identifier**
- **Site_Identifier**

## Site Groups

- **Group**
- **Site 1 thru 12**

# Fabric Help Section

## BGP Route Reflectors

**Notes:** This Section will assign the Spines to be used as Route Reflectors for the Site. This should typically be all spines at the Site(s). This Section is required.

- **Type** [Required] – The Script will run on this section if the type is set to bgp_rr. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign this Route Reflector configuration to.
- **Node_ID** [Required] – Node ID of the Spine to Assign as a Route Reflector.

## DNS Resolution Management Domain

**Notes:** For the APIC's and the Nexus Gear in the Site(s); should inband or oob be used for DNS Resolution? This Section is required if you want DNS Resolution to work. Remove the dns_mgmt Attribute to ignore this Section.

- **Type** [Required] – The Script will run on this section if the type is set to dns_mgmt. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign this DNS resolution configuration to.
- **Mgmt_Domain** [Required] – Select the inband or oob mgmt domain for DNS resolution.

# DNS Servers

**Notes:** ACI only supports up to two DNS Servers per Site. This Section is required if you want DNS Resolution to work. Remove the dns Attribute to ignore this Section.

- **Type** [Required] – The Script will run on this section if the type is set to dns. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the DNS server configuration to.
- **DNS_IP** [Required] – Currently the Script only supports IPv4 Addresses.
- **Preferred** [Required] – To assign a preferred Priority to a DNS server set this to yes. It is not required to have a preferred server.

# Domains and Search Domains

**Notes:** Domains will be added as search domains. This Section is required if you want DNS Resolution to work. Remove the domain Attribute to ignore this Section.

- **Type** [Required] – The Script will run on this section if the type is set to domain. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the Domain configuration to.
- **Domain** [Required] – A Domain that should be added as a search domain.
- **Default_Domain** [Required] – The default domain will determine which domain to use as the FQDN. Only one domain can be the Default_Domain per Site.

# NTP Servers

**Notes:** This Section is used to define NTP Servers to Assign to the Site(s). There is not a limit like DNS Servers. This Section is required. The First Line must have the ntp Attribute in the Section. Other lines can be blank.

- **Type** [Required] – The Script will run on this section if the type is set to ntp. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the NTP Server configuration to.
- **NTP_Server** [Required] – Currently the Script only supports assigning the NTP server as an IPv4 Addresses.
- **Preferred** [Required] – To assign a preferred Priority to a NTP server set this to yes. Only one should be preferred.
- **Mgmt_Domain** [Required] – Select the inband or oob mgmt domain for reaching the NTP Server.

# Smart Call Home

**Notes:** The Contract ID, Customer Identifier, and Site Identifier are defined in the Sites Tab, with the hopes that the rest of the information below should be the same for all Sites. This Section is Recommended. Remove the smartcallhome Attribute to ignore this Section.

- **Type** [Required] – The Script will run on this section if the type is set to smartcallhome. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign this Smart Callhome configuration to.
- **SMTP_Port** [Required] – TCP Port used to reach the SMTP Server. This is typically 25.
- **SMTP_Relay** [Required] – SMTP Server to send mail through.
- **Mgmt_Domain** [Required] – Select the inband or oob mgmt domain for sending mail.
- **From_Email** [Required] – The Email address to use for the from field.

- **Reply_Email** [Required] – The Email address to use for the reply field. This can be different than the from field.

- **To_Email** [Required] – The Email address to send to.

- **Phone_Number** [Optional] **–** Typically the Phone Number of the Help Desk for Network Operations. The format should include the Country Code.

- **Contact_Info** [Optional] **–** A Name or Group to use when contacting.

# SNMP Clients (Access Control)

**Notes:** Define SNMP Clients to Assign to the Site(s). This Section is required if you want to use SNMP Clients. Remove the snmp_client Attribute to ignore this Section.

- **Type** [Required] – The Script will run on this section if the type is set to snmp_client. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.

- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the SNMP Client configuration to.

- **SNMP_Client_Name** [Required] – A Name to Assign to the SNMP Client.

- **SNMP_Client** [Required] – Currently the Script only supports assigning the SNMP Client as an IPv4 Addresses.

- **Mgmt_Domain** [Required] – Select the inband or oob mgmt domain for reaching the SNMP Client.

# SNMP Communities

**Notes:** Define SNMP Clients to Assign to the Site(s). This Section is required if you want to use SNMP Clients. Remove the snmp_client Attribute to ignore this Section.

- **Type** [Required] – The Script will run on this section if the type is set to snmp_comm. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the SNMP Community configuration to.
- **SNMP_Community** [Required] – Community String.
- **Description** [Optional] – A description for the community.

# SNMP Information

**Notes:** The SNMP Trap Configuration Section is required if you want to define SNMP Traps. Remove the snmp_trap Attribute to ignore a line.

- **Type** [Required] – The Script will run on this section if the type is set to snmp_info. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the SNMP Trap Server configuration to.
- **Trap_Server** [Required] – Currently the Script only supports an IPv4 Address.
- **Destination_Port** [Required] – UDP Port for the SNMP trap destination.
- **Version** [Required] – SNMP Version to Use.
- **Community_or_Username** [Required] – Community for v1/v2c and Username for v3.
- **Security_Level** [Required] – For Security Level: Authentication and no privacy = auth [v3 only], No authentication and no privacy = noauth [v1|v2c|v3], Authentication and privacy = priv [v3 only].
- **Mgmt_Domain** [Required] – Select the inband or oob mgmt domain for sending traps.

# SNMP Users

**Notes:** The SNMP User Configuration Section is required if you want to define SNMP Users. Remove the snmp_user Attribute to ignore this Section.

- **Type** [Required] – The Script will run on this section if the type is set to snmp_user. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign this Smart Callhome configuration to.
- **SNMP_User** [Required] – Username for this SNMP User.
- **Privacy_Type:** Optional**.** SMTP Server to send mail through.
- **Privacy_Key:** Optional**.** The Privacy Key must be 8 or more characters if used.
- **Authorization_Type** [Required] – The Email address to use for the from field.
- **Authorization_Key** [Required] – The Authorization Key must be 8 or more characters if used.

# Syslog Destination Group

Notes: Syslog Destination Group Configuration. Remove the syslog_dg Attribute to ignore this Section.

- **Type** [Required] – The Script will run on this section if the type is set to syslog_dg. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign this Syslog Destination Group configuration to.
- **Dest_Grp_Name** [Required] – A Name for the Destination Group. default works but you can change to what you want it to be.
- **Minimum_Level** [Required] – What is the minimum level to include with the logs. Critical is the default but we recommend informational.
- **Log_Format** [Required] – Choose whether you want the logs to be sent in NX-OS format or ACI Format.

- **Console** [Required] – Enable or disable console logging on the switches.
- **Console_Level** [Required] – Select the console logging level.
- **Local** [Required] – Enable or disable local logging on the switches.
- **Local_Level** [Required] – Select the local logging level.
- **Include_msec [**[Required] – Include msec in the log timestamp. true or false.
- **Include_timezone** [Required] – Include the local time zone in the log timestamp. true or false.
- **Audit** [Required] – Set to true if you want to include audit logs in the syslog export. Default is false. We recommend it to be true.
- **Events** [Required] – Set to true if you want to include Events logs in the syslog export. Default is false. We recommend it to be true.
- **Faults** [Required] – Set to true if you want to include Faults logs in the syslog export. Default is true. We recommend it to be true.
- **Session** [Required] – Set to true if you want to include Session logs in the syslog export. Default is false. We recommend it to be true.

# Remote Syslog Destinations

**Notes:** Remote Syslog Destination Configuration. Remove the syslog_rmt Attribute to ignore this Section... But if any are defined the first line must have the attribute.

- **Type** [Required] – The Script will run on this section if the type is set to syslog_rmt. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign this Remote Syslog Destination configuration to.
- **Dest_Grp_Name** [Required] – A Name for the Destination Group. default works but you can change to what you want it to be.
- **Syslog_Server** [Required] – Currently the Script only supports an IPv4 Address.
  **Port** [Required] – Specify the remote port. 514 is the default.
- **Mgmt_Domain** [Required] – Select the inband or oob mgmt domain for sending syslog to the server.

- **Severity** [Required] – Select the severity level.
- **Facility** [Required] – Select the Facility of the remote server files.

# Access Help Section

## VLAN Pools

**Notes:** You Can Add more VLAN Pools but leave the defaults (access, dynamic, inband, l3out, msite) for each site, unless you are really against it and want to change what the script uses for the AAEP Policies, for example. Remove the vlan_pool Attribute to ignore a line.

**The Multi-Site VLAN pool, "msite", must be assigned VLAN 4. This is a requirement for Multi-Site. Do not change this. You can assign this same pool to all sites, without any modification.

- **Type** [Required] – The Script will run on this section if the type is set to vlan_pool. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.

- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the VLAN Pool configuration to.

- **Name** [Required] – Name of the VLAN Pool.

- **Allocation_Mode** [Required] – Set the VLAN Pool to static for physical port configuration and dynamic for VMM based integrations.

- **VLAN_Grp1** [Required] – VLAN Groups support multiple ranges i.e., "1-10,20-30,40,50" **VGRP1_Allocation** [Required] – Set the VLAN Group to static for physical port configuration and dynamic for VMM based integrations.

- **VLAN_Grp2:** [Optional] **–** The VLAN Pool Allocation Type, at times, may not match the vlan allocation mode. Thus, there are two VLAN Groups to Assign VLANs to the Pool. Only one is required.

- **VGRP2_Allocation:** [Optional] **–** Set the VLAN Group to static for physical port configuration and dynamic for VMM based integrations.

# Create Access Interface Policy Groups

*****Important Notes*****

Leave the "inband" at a minimum.  It is needed for the APIC inband Assignments.

Only Create Access Policy Groups.  VPC and Port-Channel Policy Groups will be automatically created when a VPC or Port-Channel is assigned to a Leaf Interface using attributes from one of the APGs created below.

Assign these access policy groups to the Interface Selector and then choose that it is a VPC Port.
Remove the add_polgrp Attribute to ignore a line... But always leave the first line with "inband" defined.

- **Type** [Required] – The Script will run on this section if the type is set to add_polgrp.  If you want a line to be ignored remove the type field on the line.  The line following the Titles must not be blank.

- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the Interface Policy Group configuration to.

- **Name** [Required] – A Name for the Access Interface Policy.

- **AAEP** [Required] – Select a AAEP created by the script from the drop down or assign your own.
  **MTU** [Required] – MTU size between 1300 and 9000.

- **Speed** [Required] – Select a speed policy from the drop down. inherit_Auto will set the speed according to the interface and optic default speed and turn on negotiate auto.  We recommend this as the default port mode most of the time.

- **CDP** [Required] – Enable or disable CDP on the interface.

- **LLDP_Rx** [Required] – Enable or disable LLDP receiving on the interface.

- **LLDP_Tx** [Required] – Enable or disable LLDP transmitting on the interface.

- **STP** [Required] – BPDU_ft_and_gd turns on Filter and Root Guard.  BPDU_ft only turns on BPDU Filter.  BPDU_gd only turns on Root Guard.  And BPDU_no_ft_or_gd has both disabled.

- **Description:** Optional.  A description for the policy group.

# Inventory Help Section

## Inband Management for Sites

**Notes:** Remember to Include the IP/Mask of the Gateway Address… Also Make sure you have added the Inband VLAN to the "inband" vlan pool on the previous Worksheet to the Site. This Section is Required.

- **Type** [Required] – The Script will run on this section if the type is set to inband_mgmt. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the Inband VLAN configuration to.
- **Inband_VLAN** [Required] – A VLAN Number to assign to the Inband Management.
- **Inband_GW** [Required] – Currently the Script only Supports IPv4. Assign the Gateway/Prefix i.e., 198.18.11.1/24.

## APIC Inband Management IP's

**Notes:** After the Script Runs the first time and creates the Workbook/Worksheets for the Leaf's that the APIC's are connected to, add the Policy_Group inband to the correct Interface Selector Ports. This Section is required.

- **Type** [Required] – The Script will run on this section if the type is set to apic_inb. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the Inband VLAN configuration to.
- **Name** [Required] – APIC Node Name.
- **Node_ID** [Required] – APIC Node ID. This will typically be between 1 and 7.
- **Inband_IP** [Required] **–** Currently the Script only Supports IPv4. Assign the IP/Prefix i.e., 198.18.11.11/24.
- **Inband_GW** [Required] – Currently the Script only Supports IPv4. Assign the Gateway 198.18.11.1.

# Add Switches to the Sites and Configure Inband and OOB Management IP's

**Notes:** Inband Management is Required, OOB Management is Optional - Although HIGHLY Recommended. This Section is Required.

- **Type** [Required] – The Script will run on this section if the type is set to switch. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the Switch to.
- **Serial** [Required] – Manufacturing Serial Number of the Switch.
- **Name** [Required] **–** Hostname for the Switch. The script will create the switch profile and leaf interface profile using the hostname.
- **Node_ID** [Required] – Unique ID used to identify the switch in the APIC. in the "Cisco ACI Object Naming and Numbering: Best Practice"; The recommendation is that the Spines should be 101-199 and leaves should start at 200+ thru 4000. As the number of spines should always be less than the number of leaves. See the Guide for further information: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b-Cisco-ACI-Naming-and-Numbering.html#id_107280.
- **Node_Type** [Required] **–** remote-leaf-wan or unspecified. Default is unspecified.
- **Pod_ID** [Required] – Unless you are configuring Multi-Pod, this should always be 1.
- **Switch_Role** [Required] – Select leaf or spine.
- **Switch_Type** [Required] – Select the Model number for the switch.
- **OOB_IP** [Optional] – Currently the Script only Supports IPv4 Addressing. Assign the interface IP, i.e., 198.18.1.101/24.
- **OOB_GW** [Optional] – Currently the Script only Supports IPv4 Addressing. Assign the Gateway, i.e., 198.18.1.1.
- **Inband_IP** [Required] – Currently the Script only Supports IPv4 Addressing. Assign the interface IP, i.e., 198.18.11.101/24.
- **Inband_GW** [Required] – Currently the Script only Supports IPv4 Addressing. Assign the Gateway, i.e., 198.18.11.1.

# Define Modules

**Notes:** This Section is only needed if you have Modular Switches…. 9396 would be the only leaf to type here… the rest are modular 9500 spines.

- **Type** [Required] **–** Select the Model of the modular switch.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the module configuration to.
- **Intf_Profile** [Required] – If you used this script to build your switch interface profile name is the same as the hostname.
- **Module 1 thru 16** [Required] – Assign the module type to the slots you have installed in your environment. Leave empty slots blank.

# VPC Domains

**Notes:** It is Recommended to use the 1st Node Id for the VPC ID unless you are using Node ID's less than 1000. Make sure each VPC Domain is unique in the Site.

- **Type** [Required] – The Script will run on this section if the type is set to vpc_pair. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the vpc domain configuration to.
- **VPC_ID** [Required] – An ID Number between 1 and 999 to Identify the VPC pair. We recommend this be equal to Nod1_ID.
- **Name** [Required] – Name of the VPC Domain.
- **Node1_ID** [Required] – The Node ID of the First Node in the group.
- **Node2_ID** [Required] – The Node ID of the Second Node in the group.

# Convert Uplinks to Downlinks

**Notes:** You May Need to remove the Interface Selector Policy Group Before Applying this Section. This is not currently supported.

- **Type** [Required] – The Script will run on this section if the type is set to port_cnvt. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the module configuration to.
- **Name** [Required] – Name of the Switch Interface Profile.
- **Node_ID** [Required] – Node ID of the Switch.
- **Port** [Required] – What Port You want to convert.

# Create BreakOut Ports

**Notes:** This is not Currently Supported. If Desired Please Provide Feedback on GitHub Repository. Right now, Manually Create the New Interface Selectors on the Corresponding Leaf Worksheet.

- **Type** [Required] – The Script will run on this section if the type is set to brk_out. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the module configuration to.
- **Intf_Profile** [Required] – Name of the Switch Interface Profile.
- **Port** [Required] – The Port number you want to convert.
- **BreakOut_Name** [Required] – Select the Break-Out Policy group from the drop down.

# Admin Help Section

## Configuration Backup

**Notes:** The Encryption Key is used to encrypt the backup files. Minimum 16 and maximum 32 characters.

- **Type** [Required] – The Script will run on this section if the type is set to backup. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the backup configuration to.
- **Encryption_Key** [Required] – A VLAN Number to assign to the Inband Management.
- **Backup_Hour** [Required] – Hour of the Day to backup. 0 thru 23. The Backup Hour and Minute are used to create a triggered schedule once per day for configuration backups.
- **Backup_Minute** [Required] – Minute of the day to backup. 0 to 59.
- **Remote_Host** [Required] – IP or Hostname of a remote host to send backup data to.
- **Mgmt_Domain** [Required] – Select either inband or oob from the management domain drop-down. This defines which domain will be used to send the backup files to the server.
- **Protocol** [Required] – Select the Protocol from the drop-down menu.
- **Remote_Path** [Required] – Remote path to place the file on the server. i.e., /tmp.
- **Port** [Required] – Remote Port of the Server.
- **Auth_Type** [Required] – Select passwd for user/pass authentication, or ssh-key: for SSH Key based authentication.
- **Username** [Optional] – Required if the Auth_Type is passwd.
- **Passwd_or_SSH_Pass** [Required] – Either assign the password for username/password authentication or the SSH passphrase for SSH based authentication.
- **SSH_Key** [Optional] – Input the SSH Private key if using SSH based authentication.
- **Description** [Optional] – A description for the import/export policy.

# RADIUS

**Notes:** After the Script Runs the first time and creates the Workbook/Worksheets for the Leaf's that the APIC's are connected to, add the Policy_Group inband to the correct Interface Selector Ports. This Section is required.

- **Type** [Required] – The Script will run on this section if the type is set to apic_inb. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the Inband VLAN configuration to.
- **Name** [Required] – APIC Node Name.
- **Node_ID** [Required] – APIC Node ID. This will typically be between 1 and 7.
- **Inband_IP** [Required] **–** Currently the Script only Supports IPv4. Assign the IP/Prefix i.e., 198.18.11.11/24.
- **Inband_GW** [Required] – Currently the Script only Supports IPv4. Assign the Gateway 198.18.11.1.

# TACACS+

**Notes:** Inband Management is Required, OOB Management is Optional - Although HIGHLY Recommended. This Section is Required.

- **Type** [Required] – The Script will run on this section if the type is set to switch. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the Switch to.
- **Serial** [Required] – Manufacturing Serial Number of the Switch.
- **Name** [Required] **–** Hostname for the Switch. The script will create the switch profile and leaf interface profile using the hostname.
- **Node_ID** [Required] – Unique ID used to identify the switch in the APIC. in the "Cisco ACI Object Naming and Numbering: Best Practice"; The recommendation is that the Spines should be 101-199 and leaves should start at 200+ thru 4000. As the number of spines should always be less than the number of leaves. See the Guide for further information:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b-Cisco-ACI-Naming-and-Numbering.html#id_107280.

- **Node_Type** [Required] **–** remote-leaf-wan or unspecified. Default is unspecified.
- **Pod_ID** [Required] – Unless you are configuring Multi-Pod, this should always be 1.
- **Switch_Role** [Required] – Select leaf or spine.
- **Switch_Type** [Required] – Select the Model number for the switch.
- **OOB_IP** [Optional] – Currently the Script only Supports IPv4 Addressing. Assign the interface IP, i.e., 198.18.1.101/24.
- **OOB_GW** [Optional] – Currently the Script only Supports IPv4 Addressing. Assign the Gateway, i.e., 198.18.1.1.
- **Inband_IP** [Required] – Currently the Script only Supports IPv4 Addressing. Assign the interface IP, i.e., 198.18.11.101/24.
- **Inband_GW** [Required] – Currently the Script only Supports IPv4 Addressing. Assign the Gateway, i.e., 198.18.11.1.

# Authentication Realm

**Notes:** This Section is only needed if you have Modular Switches…. 9396 would be the only leaf to type here… the rest are modular 9500 spines.

- **Type** [Required] **–** Select the Model of the modular switch.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the module configuration to.
- **Intf_Profile** [Required] – If you used this script to build your switch interface profile name is the same as the hostname.
- **Module 1 thru 16** [Required] – Assign the module type to the slots you have installed in your environment. Leave empty slots blank.

# Web Security

**Notes:** Typically, the only setting I change is settings the Web_Timeout to the Maximum 65525 and Enforce_Intv to disabled, but neither are recommended best practice. Modify if your org requires tighter security policies.

- **Type** [Required] – The Script will run on this section if the type is set to web_security. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Passwd_Strength** [Required] – Password Strength Check: Should the APIC Validate the Complexity of Password: Default is true.
- **Enforce_Intv** [Required] – Enforce Password Change Interval: Default is Enable.
- **Passwd_Intv** [Required] – Change Interval (hours): Between 0 and 745 Hours. Default is 48
  **Number_Allowed** [Required] – Number of changes allowed within the change interval (changes): Between 0 and 10. Default is 2.
- **Passwd_Store** [Required] – Number of recent user password to store: Between 0 and 15. Default is 5.
- **Lockout:** Lockout User after multiple failed login attempts: Default is Disable.
- **Failed_Attempts** [Required] – Number of failed attempts before user is locked out. Between 1 and 15. Default is 5 if Lockout is enabled.

- **Time_Period** [Required] – Time period in which consecutive attempts were failed (m): Between 1 and 720 minutes. Default is 5 Minutes if Lockout is enabled.

- **Dur_Lockout** [Required] – Duration of lockout (m): Between 1 and 1440. Default is 60 Minutes if Lockout is enabled.

- **Token_Timeout** [Required] – Web Token Timeout (s): How Long to Allow REST API Token Validity: Between 300 and 9600 seconds. Default is 600.

- **Maximum_Valid** [Required] – Maximum Validity Period (h): Between 0 and 24: Default is 24 Hours.

- **Web_Timeout** [Required] – The Web Session Idle Timeout can be between 60 and 65525 seconds. The Default is 1200 seconds.

# Tenants Help Section

## Create Tenants

**Important Notes**

Keep your names simple. It will save you time when troubleshooting. Most CLI commands have a 10-character limit on the display field. So, if your VRF Name is longer than 10 characters it will wrap and be harder to read.

- **Type** [Required] – The Script will run on this section if the type is set to add_tenant. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.

- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the Tenant configuration to.

- **Tenant** [Required] – Tenant Name can be up to 64 alphanumeric characters + underscore "_" or dash "-". But we recommend keeping it under or equal to 10 characters.

- **Description** [Optional] – Currently the Script only Supports IPv4. Assign the Gateway/Prefix i.e., 198.18.11.1/24.

# VRF Help Section

## Create VRF's

**Important Notes**

Keep your names simple. It will save you time when troubleshooting. Most CLI commands have a 10-character limit on the display field. So, if your VRF Name is longer than 10 characters it will wrap and be harder to read.

We Recommend Putting the VRFs in the Common Tenant, to simplify routing between VRFs (if ever desired now or in the future), it will save you time from having to create import/export route control policies.

Many Integrations also need the VRF in the Common Tenant, like Kubernetes CNI.

- **Type** [Required] – The Script will run on this section if the type is set to add_vrf. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign this VRF configuration to.
- **Tenant** [Required] – Name of the Tenant.
- **VRF** [Required] – Name of the VRF.
- **Description** [Optional] – Description for the VRF.
- **VRF Policy** [Required] – This must be pre-defined in the "Network Policies" Worksheet. Please refer to the Network Polices help section for more details.

## Create SNMP Context Communities

****Important Notes****

This Section is only necessary if you want a "SNMP Context Community" Defined. An SNMP Context was created as part of the VRF Creation.

Note: A Community can only be used within the context when assigned to it. But a Fabric Wide SNMP Community can be used for an SNMP Context when qualified with the Context.

- For Example, to get Inband IPv4 Management Address without an SNMP Community assigned to the VRF SNMP Context you would do:

```
[tyscott@lnx1 ~]$ snmpwalk -c isitgoodenough@inb -v2c asgard-
leaf101.rich.ciscolabs.com ipAddressPrefixOrigin.335544322.ipv4
IP-MIB::ipAddressPrefixOrigin.335544322.ipv4."192.168.169.251".32 =
INTEGER: manual(2)
[tyscott@lnx1 ~]$
```

inb is the name of the context created by the script for VRF inb. To Query the Same parameter with a Community assigned to the inb Context you would do:

```
[tyscott@lnx1 ~]$ snmpwalk -c walkthisway -v2c asgard-
leaf101.rich.ciscolabs.com ipAddressPrefixOrigin.335544322.ipv4
IP-MIB::ipAddressPrefixOrigin.335544322.ipv4."192.168.169.251".32 =
INTEGER: manual(2)
[tyscott@lnx1 ~]$
```

Note that "walkthisway" can only be used with the "inb" SNMP Context since it is assigned to it, while the community "isitgoodenough" can be used Fabric wide.

See SNMP Configuration Guide: https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/aci-guide-configuring-snmp.pdf for more information

Note: The Context_Community Field is Hidden but displays in the Formula Bar when the cell is selected

- **Type** [Required] – The Script will run on this section if the type is set to ctx_comm. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign this VRF configuration to.
- **Tenant** [Required] – Name of the Tenant.
- **VRF** [Required] – Name of the VRF.
- **Description** [Optional] – Description for the Context Community.
- **Ctx_Community** [Required] – This is a Community string to add to the context. The same rules apply as for the fabric community string length.

# L3Out Help Section

## Add Switches to the Sites and Configure Inband and OOB Management IP's

**Notes:** Inband Management is Required, OOB Management is Optional - Although HIGHLY Recommended. This Section is Required.

- **Type** [Required] – The Script will run on this section if the type is set to switch. If you want a line to be ignored remove the type field on the line. The line following the Titles must not be blank.
- **Site_Group** [Required] – Assign either the individual site or a group of sites to assign the Switch to.
- **Serial** [Required] – Manufacturing Serial Number of the Switch.
- **Name** [Required] **–** Hostname for the Switch. The script will create the switch profile and leaf interface profile using the hostname.
- **Node_ID** [Required] – Unique ID used to identify the switch in the APIC. in the "Cisco ACI Object Naming and Numbering: Best Practice"; The recommendation is that the Spines should be 101-199 and leaves should start at 200+ thru 4000. As the number of spines should always be less than the number of leaves. See the Guide for further information: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b-Cisco-ACI-Naming-and-Numbering.html#id_107280.
- **Node_Type** [Required] **–** remote-leaf-wan or unspecified. Default is unspecified.
- **Pod_ID** [Required] – Unless you are configuring Multi-Pod, this should always be 1.
- **Switch_Role** [Required] – Select leaf or spine.
- **Switch_Type** [Required] – Select the Model number for the switch.
- **OOB_IP** [Optional] – Currently the Script only Supports IPv4 Addressing. Assign the interface IP, i.e., 198.18.1.101/24.
- **OOB_GW** [Optional] – Currently the Script only Supports IPv4 Addressing. Assign the Gateway, i.e., 198.18.1.1.
- **Inband_IP** [Required] – Currently the Script only Supports IPv4 Addressing. Assign the interface IP, i.e., 198.18.11.101/24.

- **Inband_GW** [Required] – Currently the Script only Supports IPv4 Addressing. Assign the Gateway, i.e., 198.18.11.1.

# Networks Help Section

## Create Networks

****Important Notes****

*** Policy is a Unique Aspect to this script related to the Policies assigned to BD, Subnet, App and EPG. In Part it is because it is unrealistic to have all the options required on one page. So, this allows to define the polices on a separate tab.**

* But at the same time, it should greatly simplify configuration for you as you can create generic policies and apply them to multiple Bridge Domains, without having to define the same settings over and over.

*** Make sure you define your policies in the "Network Polices" Tab before running the script.**

- **Type** [Required] **–** This will always be add_net.
- **Site_Group** Required. Assign either the individual site or a group of sites to assign this Network configuration to.
- **Tenant** [Required] **–** Tenant Name.
- **Bridge_Domain** [Required] **–** Bridge Domain Name.
- **BD_Description** [Optional] **–** A Description for the Bridge Domain.
- **BD_Policy** [Required] **–** This is defined on the "Network Policies" Worksheet.
- **VRF** [Required] **–** Name of the VRF.
- **Subnets** [Optional] **–** IP/Mask of the Gateway Interface used for the Subnet. This will configure the Anycast Gateway.
- **Subnet_Description** [Optional] **–** a Description for the subnet.
- **Subnet_Policy** [Optional] **–** Only required if Subnet is defined. This is defined on the "Network Policies" Worksheet.
- **L3Out_Policy** [Optional] **–** Only required if Subnet is defined. The Policy Table will define the L3Out Name per Site.
- **App_Profile** [Required] **–** Name of the Application Profile. We recommend keeping this name under 10 characters.

- **App_Policy** [Required] **–** This is defined on the "Network Policies" Worksheet.
- **EPG** [Required] **–** Name of the EPG. We recommend keeping this name under 10 characters.
- **EPG_Description** [Optional] **–** A description for the EPG.
- **EPG_Policy** [Required] **–** This is defined on the "Network Policies" Worksheet.
- **VLAN** [Required] **–** VLAN to use for static port mapping with this vlan.
- **PVLAN** [Optional] **–** Private VLAN to use for static port mapping with this vlan. Optional. Only required for Private VLAN Configurations

# Network Policies Help Section

## 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