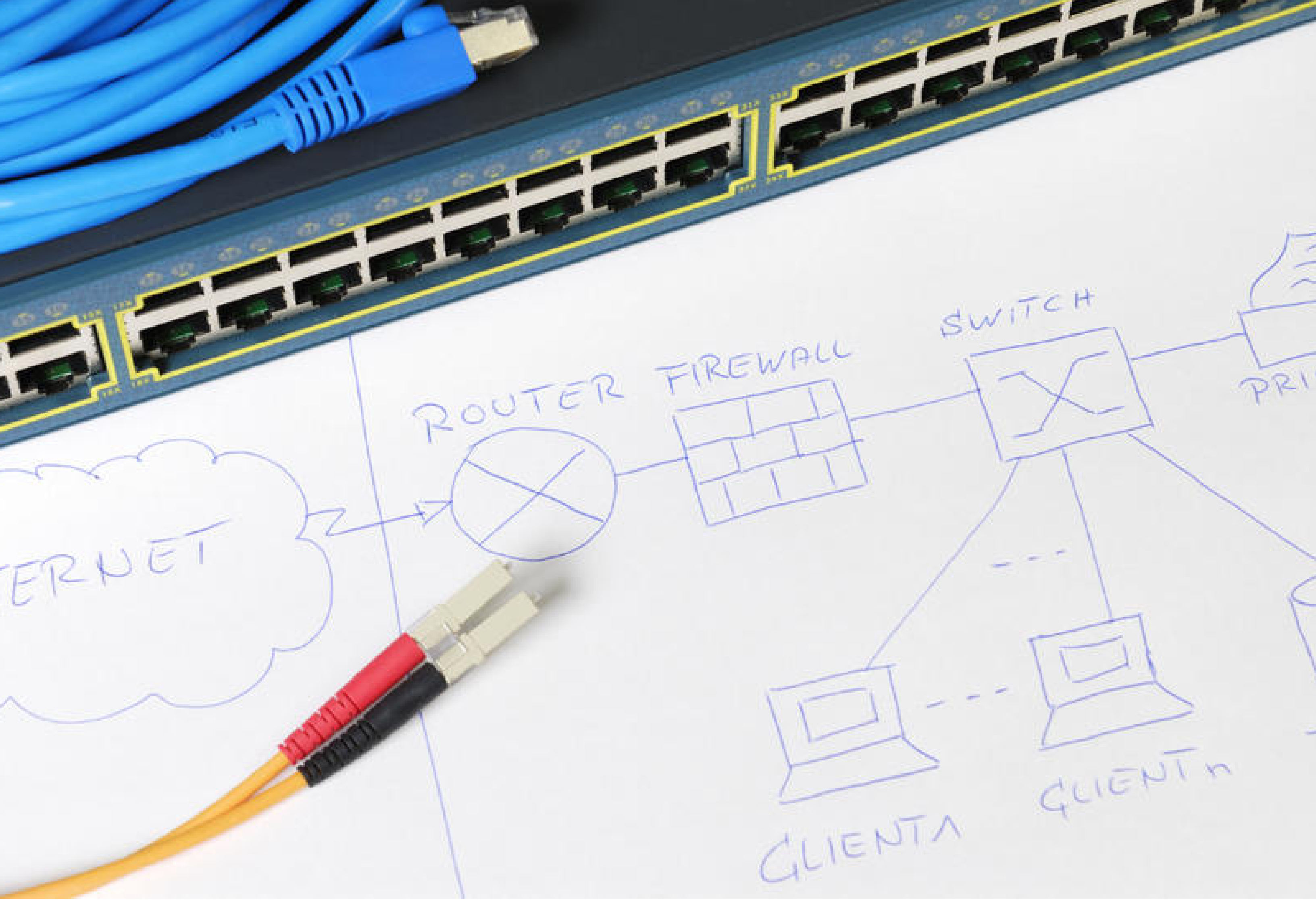


Network Design Cookbook

2nd Edition

Michel Thomatis, CCIE #6778
RouteHub Group, LLC
www.RouteHub.net

Version 2.0.4 (December 2017)

CISCO CERTIFIED
CCIE
15 YEARS

Network Design Cookbook – 2nd Edition

by

Michel Thomatis, CCIE #6778

May 8, 2011

About the Author

Michel Thomatis, CCIE #6778 (15 year) - Chief Network Architect & Lead Trainer

Michel has spent the last 18 years as a network engineer/architect. As a 15-year CCIE, Michel loves the opportunity to provide training in a wide-array of network technologies. He formerly worked at Cisco, as well as in government, banking, and non-profit organizations. He has published the “Network Design Cookbook” and a science fiction novel called “The Dark End”. He has also published various iOS applications (virtual Network Engineer, Circlefalls) that can be found on Apple’s iOS App Store. Other software development experience includes python and SDN. Currently, Michel is the owner, Chief Network Architect and Lead Trainer at RouteHub Group, LLC.

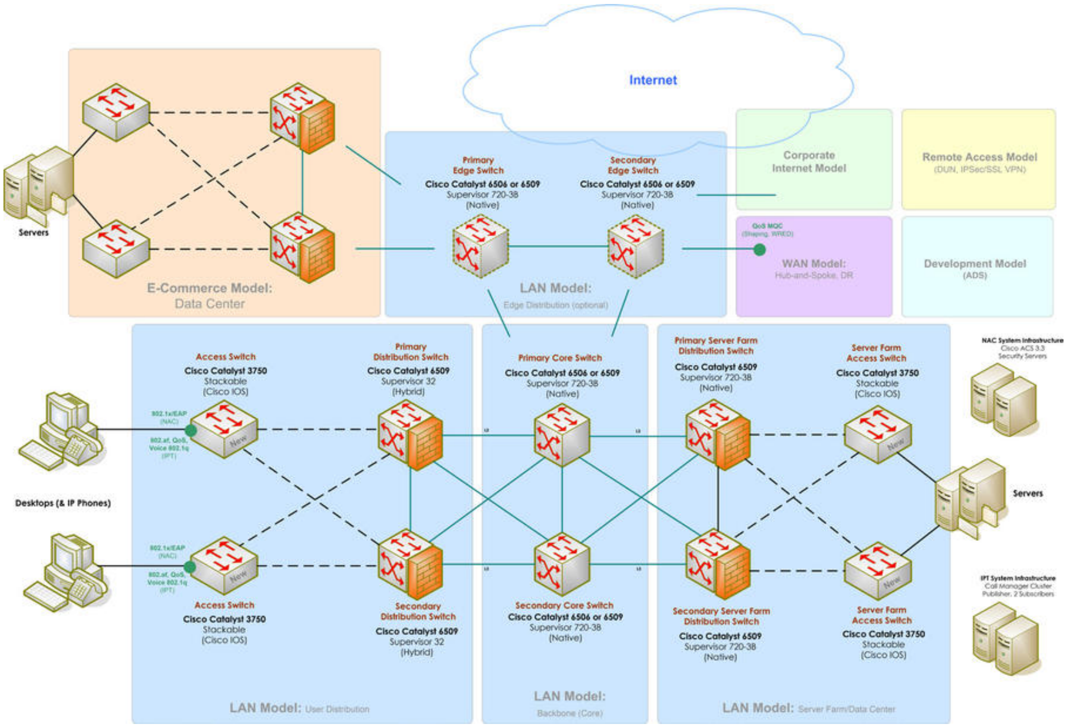
Table of Contents

Start Here

Introduction

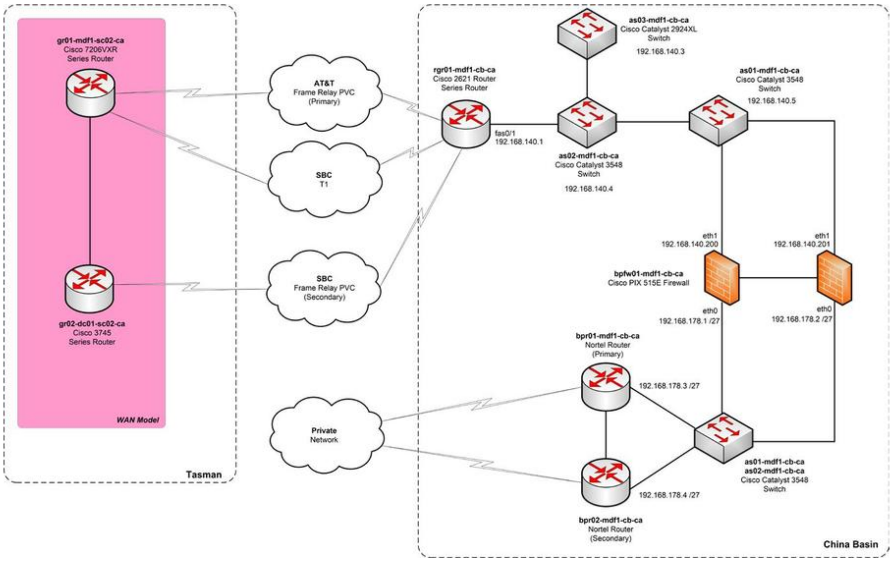
Before you get started, I want to talk about how to use and navigate throughout the design cookbook in this new edition. The network design cookbook has been a personal project on mine ever since I started out in the networking field more than 20 years ago. My biggest personal attributes have always been with structure and organization. I constantly try to build structure and organize every aspect that I interactive with. Especially in areas that I am deeply passionate about such as networking. The biggest problem that I saw in the networking field at the time, including today, is the lack of structure to build and design networks.

Here is one of my earlier attempts to establish a network design standard:



It involved selecting design modules and connecting them together based on what was required. I continued this approach for several years which eventually evolved into the first edition of the network design cookbook.

However, I wanted to improve on this structure further and I determined the root issue that my design cookbook never addressed .... why do network diagrams look so different from one another?



I have seen hundreds of diagrams over the years. Many of them I have always pondered on what the diagram was trying to accomplish and why it was so different from what I would typically do.

I wanted the ability to provide a design structure that could be used to build a network design in several different ways to mirror what could be produced with the different design diagrams out there. This required me to look deeper into the problem to determine why network designs were not universally the same. And it didn't take long to figure out exactly what was going on. With the hundreds of diagrams that I have seen, many of them I agreed with the approach taken. While there were other diagrams that I always questioned. Well, the answer was quite simple. Those designs I questioned were built in a way that I would never do. And the diagrams that I agreed with simply mirrored what I would typically design.

That doesn't mean that the other diagrams were designed incorrectly, it only shows that there are many ways to complete a network design. This was something I touched upon briefly in the first edition of the network design cookbook.

A network design will be based on three main aspects: Requirements, Recommendations, and Preferences

The individuals involved in the design process will typically be the following:

- Business Owner / Management / Other
- Engineer / Administrator / Technician

The requirements will typically come from the business owner, management, or some other group. They will tell you what they need accomplish such as Internet access or that the users need to access a server located at a different office. They will typically not give you any recommendations or preferences.

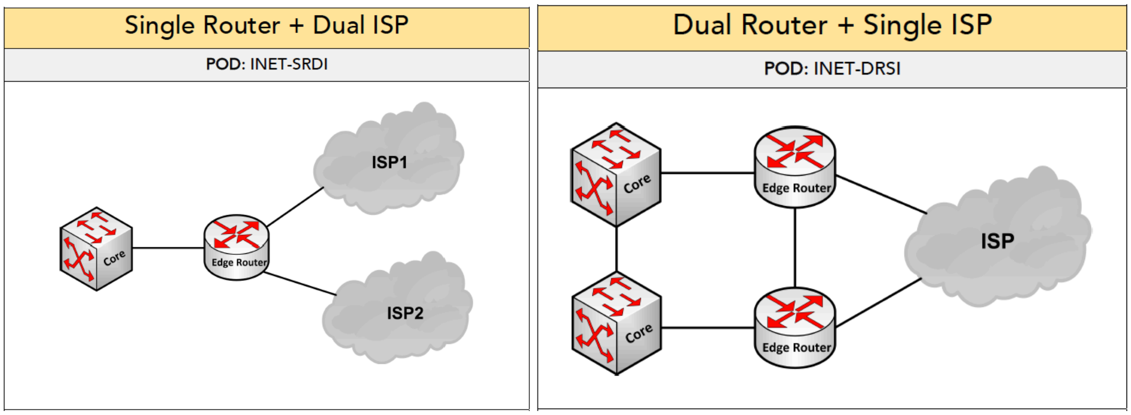
The recommendations and preferences will typically come from the network architect/engineer who is tasked to build the design. These will be based on that engineer's experience and what has worked for them in the past including their current skill set. They will have preferences for the type of hardware that should be used to even the type of topology that will be deployed.

For example, I have met network engineers who were very fearful of any Layer-2 configuration involving VLANs, Trunking, to the dreadful Spanning Tree Protocol. I say dreadful because those network engineers suffered major broadcast storm outages that brought down the entire network. That is considered as an experience that the engineer will avoid at all cost in the future. Therefore, all of their designs will involve a Layer-3 only topology with limited Layer-2 configuration. From their perspective, they would not recommend using Layer-2 topologies due to possible broadcast storms. They are speaking from experience and that will dictate the type of design they will deploy moving forward.

For me, I recommend Layer-2 topologies if the requirement calls for it. I have seen broadcast storms in the past due to misconfiguration on the network switches. Again, based on my experience as a network engineer.

This is the main reason that one design will be different from the next. The design will vary based on the recommendations and the preferences of the network engineer who is building that design. With that understanding, I revisited my design modules approach and organized it in a way that a network engineer can make a choice for which module to use based on the business requirements and their own professional preferences.

Here is an example for one of these design PODs and what they can provide:



This shows two Internet PODs and what that specific topology looks like. One POD shows one edge router connecting to two ISP clouds and another POD shows one ISP cloud connected to dual edge routers. If you believe that the ISP is typically the root cause for issues then the single router dual ISP POD is what you may consider. If you believe that the router hardware is the likely cause of any issue, then you may consider the dual router with single ISP POD for the Internet topology.

There are other PODs listed providing different scenarios that can be considered. In a nutshell, that is the structure of the network design cookbook recognizing that each design can be different.

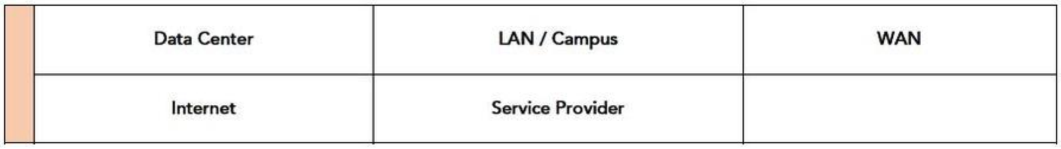
With that discussed let's dive in and explain the design structure at a high-level and how it is integrated within the design cookbook.

Design Process

The network design cookbook is broken up into several sections in numbered order and below reflects the flow for how a design should be completed:

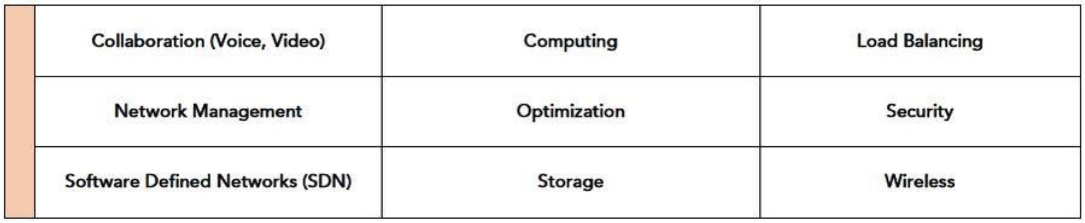
- Framework
- Solutions
- Services
- Attributes

You first start off by building the framework of the network which can be a LAN, Data Center, WAN, Internet, and/or Service Provider. All other solutions and services will overlay on-top of the framework. You can treat the framework as the structure of a house. You can't put in the kitchen and furniture until the structure of the house is built.



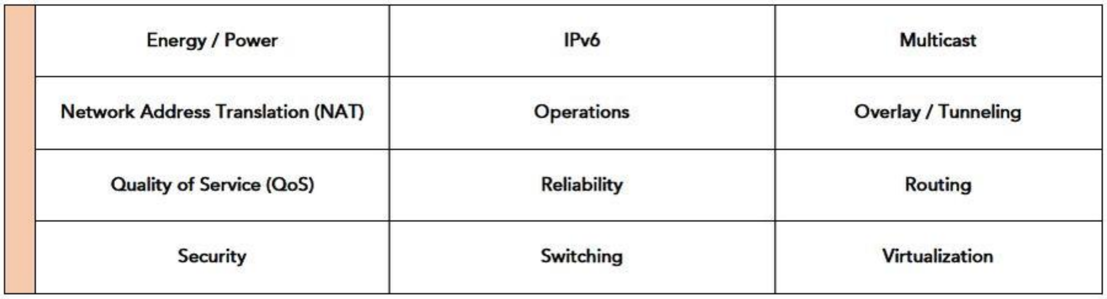
Data Center	LAN / Campus	WAN
Internet	Service Provider	

Once you complete the framework, you need to determine what other solutions will be used on-top of this framework to provide a certain capability to the environment. These solutions can include Voice, SDN, Firewall, to maybe WAN optimization. You can treat "Solutions" like the actual rooms in the house such as the kitchen, living room, bedroom, to several bathrooms if needed.



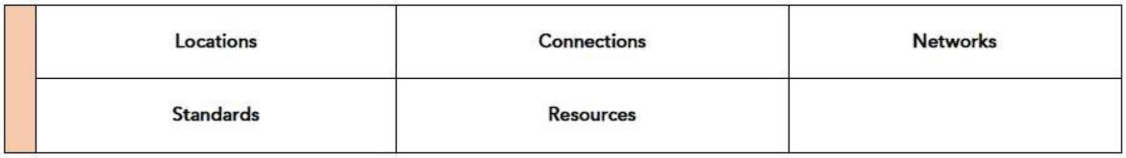
Collaboration (Voice, Video)	Computing	Load Balancing
Network Management	Optimization	Security
Software Defined Networks (SDN)	Storage	Wireless

Next, you want to determine what services will be deployed on-top of the framework and solutions previously determined. These services can include Routing, Switching, VPN, to SNMP among others. You can treat services like the actual furniture that exist inside the various rooms in the house such as chairs, tables, a bed, stove, and so on.



Energy / Power	IPv6	Multicast
Network Address Translation (NAT)	Operations	Overlay / Tunneling
Quality of Service (QoS)	Reliability	Routing
Security	Switching	Virtualization

As you navigate your way through the design from foundation, solutions, then to services you will need to consider what attributes the network will have. This isn't something that is done first or last, but in conjunction (when needed) along the way. This will include attributes such as naming standards, IP addressing standards, to what type of bandwidth services will be used between the various components in the design. Using our house example, this would be how each room is organized and knowing where to find something. For example, one cabinet in the kitchen will hold all glasses and another cabinet will hold all pots & pans. This can be extremely valuable because if we need to locate something, we know exactly where to go within the house to get it.



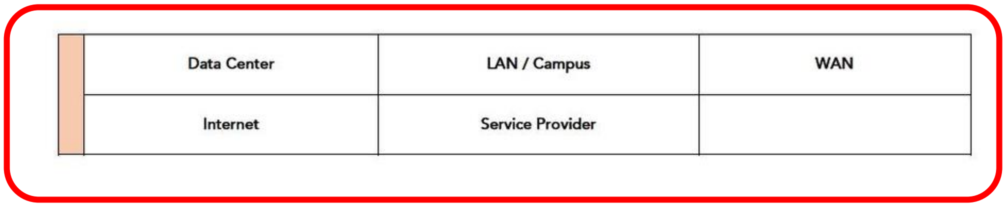
Locations	Connections	Networks
Standards	Resources	

Design PODs

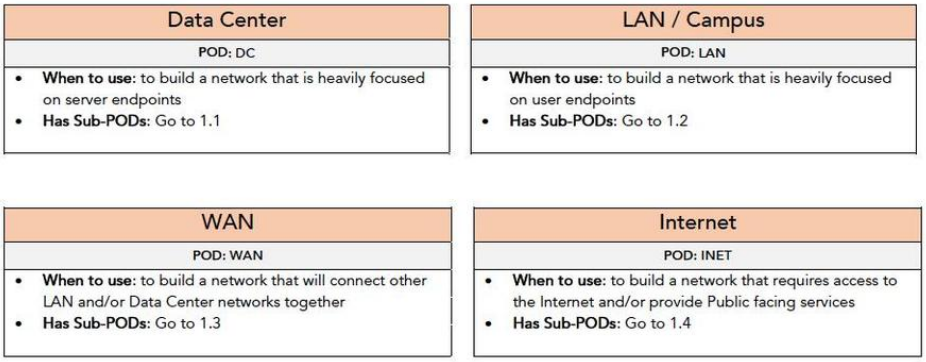
Now that you understand the design process, let's go deeper and talk about what you will see in those sections. Everything will be represented as a POD and there is different type of PODs that will be used in design cookbook:

- Summary POD
- Basic POD
- Advanced POD
- Grid POD
- Configuration POD

A ***Summary POD*** will show all possible design PODs we can choose from. Some of the frameworks, solutions, and services will have several PODs, so this can provide a type of legend for knowing all possible PODs within that section. Below shows a summary of all possible Frameworks we can use:



Data Center	LAN / Campus	WAN
Internet	Service Provider	



Data Center

POD: DC

- **When to use:** to build a network that is heavily focused on server endpoints
- **Has Sub-PODs:** Go to 1.1

LAN / Campus

POD: LAN

- **When to use:** to build a network that is heavily focused on user endpoints
- **Has Sub-PODs:** Go to 1.2

WAN

POD: WAN

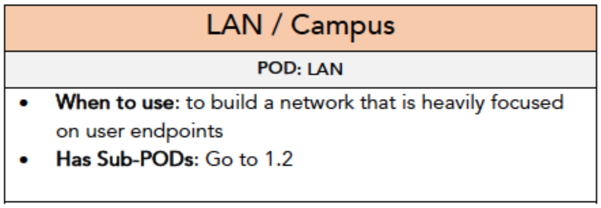
- **When to use:** to build a network that will connect other LAN and/or Data Center networks together
- **Has Sub-PODs:** Go to 1.3

Internet

POD: INET

- **When to use:** to build a network that requires access to the Internet and/or provide Public facing services
- **Has Sub-PODs:** Go to 1.4

Another type of POD in its simplest form is called a "***Basic POD***". There are other PODs that look like this and will provide more information that we can use. Within this POD you will see three sections. There is the title, the POD ID, and design items.



LAN / Campus

POD: LAN

- **When to use:** to build a network that is heavily focused on user endpoints
- **Has Sub-PODs:** Go to 1.2

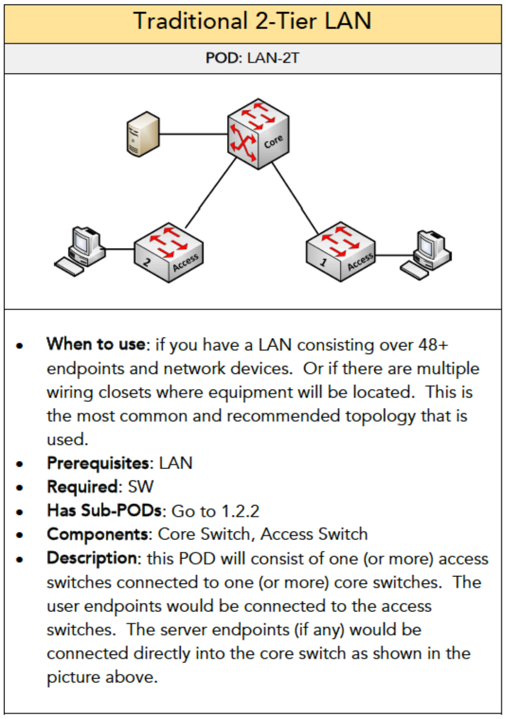
The title reflects the name for that actual POD. The POD ID is how this design POD is identified within the design cookbook. This information is important because some PODs may require other PODs to be selected first.

The design items will present a series of questions or resources that we can reference to determine if this POD is needed or not. This type of POD will have a "When to use". This will outline the best scenario or use-case for choosing that POD. This item provides the greatest value and proves why network designs can be different.

There is another item called "Sub-PODs". This means there are additional design PODs that need to be looked at and chosen for the overall network design. It may be informational or provide details for how the design should be deployed.

Bringing all of this together and looking at an example Basic POD, this POD is for a LAN / Campus framework. Its POD ID is "LAN". We should use this POD if we are building a network that will be heavily focused on user endpoints. Therefore, if this POD will be used, we need to go to section 1.2 to continue building the LAN design.

This will lead us to another POD type called the "***Advanced POD***" as shown below:



Traditional 2-Tier LAN

POD: LAN-2T

- **When to use**: if you have a LAN consisting over 48+ endpoints and network devices. Or if there are multiple wiring closets where equipment will be located. This is the most common and recommended topology that is used.
- **Prerequisites**: LAN
- **Required**: SW
- **Has Sub-PODs**: Go to 1.2.2
- **Components**: Core Switch, Access Switch
- **Description**: this POD will consist of one (or more) access switches connected to one (or more) core switches. The user endpoints would be connected to the access switches. The server endpoints (if any) would be connected directly into the core switch as shown in the picture above.

This will mirror the Basic POD, but it will provide a lot more details. The most noticeable addition is the diagram picture. This shows a picture of the actual topology that is being referenced in the design POD. This can provide us a picture that we can draw out and connect with other PODs that we chose along the way.

Besides the diagram picture being included in the Advanced POD, it will show other design items such as Prerequisites, Required, Components, and Description.

- **Prerequisites** means that one (or more) other design PODs are required before selecting this POD. It will show the actual POD(s) based on its ID.
- **Required** means what other PODs must be added to our design process to be completed
- **Components** reflects the main network devices that are used in the POD and referenced in the diagram picture

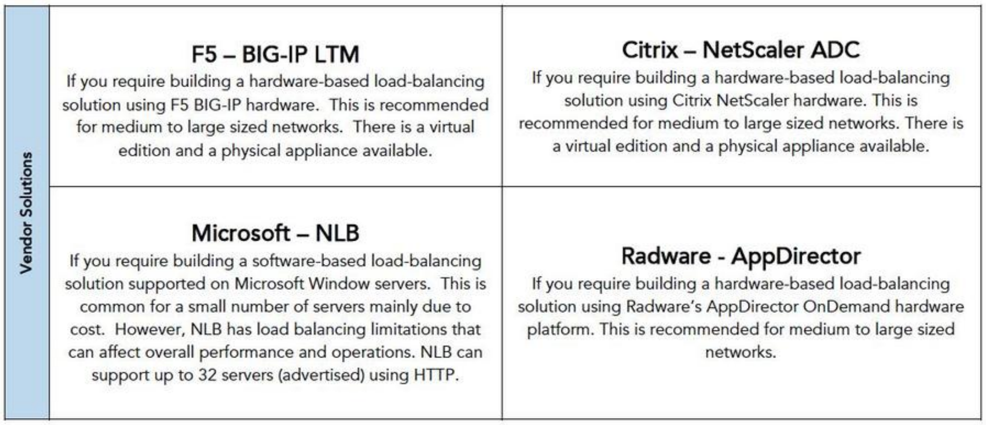
- **Description** explains the actual topology that is used in the POD and what is shown in the diagram picture for reference

Bringing all of this together, this is a LAN Advanced POD for a Traditional 2-Tier LAN with a POD ID of LAN-2T. We should use this POD if our LAN will consist of 48+ endpoints. Or if there will be multiple wiring closets where the network equipment will be located.

In order to use this POD, we must select the "LAN" POD which is why we are here to begin with. And using this POD will require the "Switching" POD (POD ID of SW).

This POD will consist of a Core switch and one (or more) access switches which we see in the provided diagram picture and outlined in the description. We also see that this POD has additional PODs that we need to look at for building our LAN. Therefore, we would need to go to section 1.2.2 within the design cookbook where other PODs will be listed.

Another type of POD is called a "***Grid POD***" as shown below:

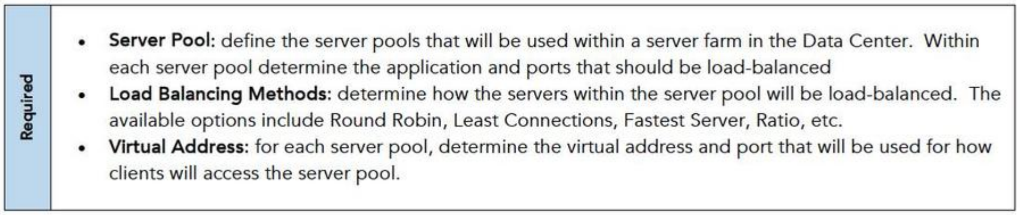


Vendor Solutions	**F5 – BIG-IP LTM** If you require building a hardware-based load-balancing solution using F5 BIG-IP hardware. This is recommended for medium to large sized networks. There is a virtual edition and a physical appliance available.	**Citrix – NetScaler ADC** If you require building a hardware-based load-balancing solution using Citrix NetScaler hardware. This is recommended for medium to large sized networks. There is a virtual edition and a physical appliance available.
	Microsoft – NLB If you require building a software-based load-balancing solution supported on Microsoft Window servers. This is common for a small number of servers mainly due to cost. However, NLB has load balancing limitations that can affect overall performance and operations. NLB can support up to 32 servers (advertised) using HTTP.	**Radware - AppDirector** If you require building a hardware-based load-balancing solution using Radware's AppDirector OnDemand hardware platform. This is recommended for medium to large sized networks.

These PODs will either list a vendor solution or maybe a general best practice. For example, in the Grid POD shown above, this will list vendor solutions that we can choose for a Load Balancing solution. It will show the vendor and the product followed by "when to use" info for consideration.

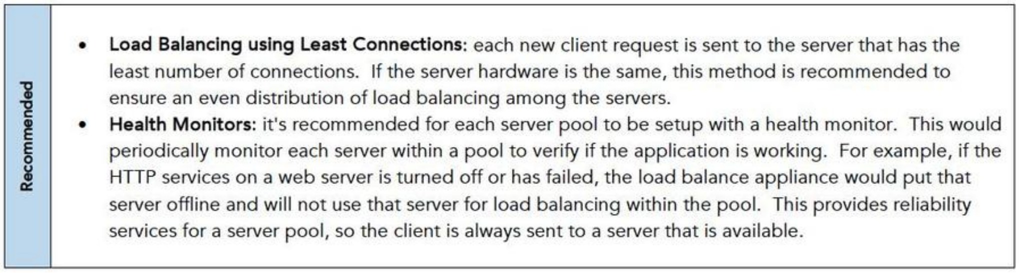
For example, if we are building a local load-balancing solution then we need to determine which vendor solution will be used for the components in that load-balancing POD. We need to select only one, so we can use the F5 BIG-IP LTM for the load-balancing component in that topology.

Another type of POD is called a "***Configuration POD***" as shown below:



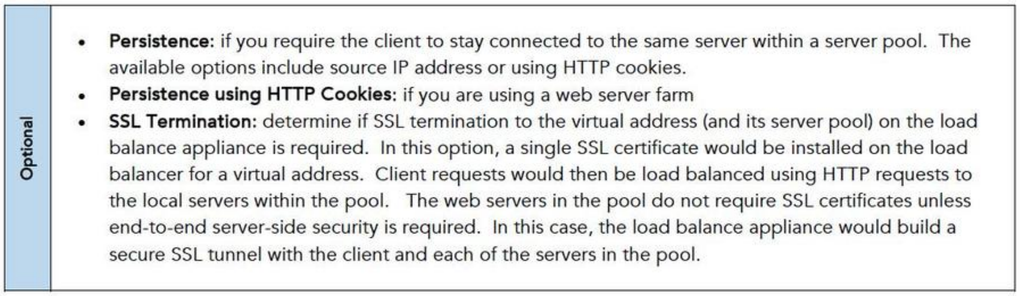
Required

- **Server Pool:** define the server pools that will be used within a server farm in the Data Center. Within each server pool determine the application and ports that should be load-balanced
- **Load Balancing Methods:** determine how the servers within the server pool will be load-balanced. The available options include Round Robin, Least Connections, Fastest Server, Ratio, etc.
- **Virtual Address:** for each server pool, determine the virtual address and port that will be used for how clients will access the server pool.



Recommended

- **Load Balancing using Least Connections:** each new client request is sent to the server that has the least number of connections. If the server hardware is the same, this method is recommended to ensure an even distribution of load balancing among the servers.
- **Health Monitors:** it's recommended for each server pool to be setup with a health monitor. This would periodically monitor each server within a pool to verify if the application is working. For example, if the HTTP services on a web server is turned off or has failed, the load balance appliance would put that server offline and will not use that server for load balancing within the pool. This provides reliability services for a server pool, so the client is always sent to a server that is available.



Optional

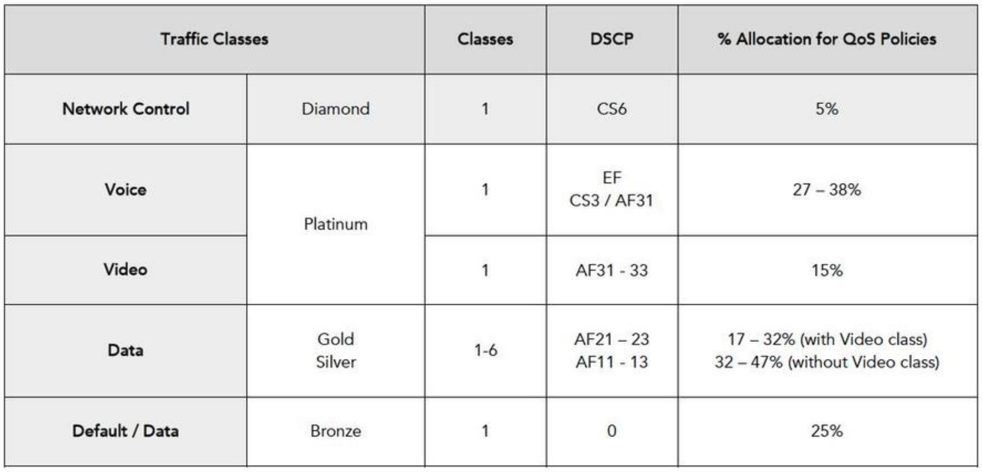
- **Persistence:** if you require the client to stay connected to the same server within a server pool. The available options include source IP address or using HTTP cookies.
- **Persistence using HTTP Cookies:** if you are using a web server farm
- **SSL Termination:** determine if SSL termination to the virtual address (and its server pool) on the load balance appliance is required. In this option, a single SSL certificate would be installed on the load balancer for a virtual address. Client requests would then be load balanced using HTTP requests to the local servers within the pool. The web servers in the pool do not require SSL certificates unless end-to-end server-side security is required. In this case, the load balance appliance would build a secure SSL tunnel with the client and each of the servers in the pool.

These will provide details for how the network devices should be configured within that POD and topology. There will be up to three type of configuration sections available:

- **Required**: this means configuration that is required on one (or more) network devices in order for it to be operational
- **Recommended**: this will provide a list of recommended configuration or best practices to add to the network devices in that POD if applicable. These are not required only recommended for increase security and stability.
- **Optional**: this will provide a list of features and options that may be used in the topology.

The Configuration POD above is from the Local Load-Balancing POD section and what you can expect.

Lastly, there will be other sections in the design cookbook that will list design concepts for various technologies such as IPv6, QoS (example below), to Security.



Traffic Classes		Classes	DSCP	% Allocation for QoS Policies
Network Control	Diamond	1	CS6	5%
Voice	Platinum	1	EF CS3 / AF31	27 – 38%
Video		1	AF31 - 33	15%
Data	Gold Silver	1-6	AF21 – 23 AF11 - 13	17 – 32% (with Video class) 32 – 47% (without Video class)
Default / Data	Bronze	1	0	25%

This will outline how to design those solutions/services by providing a unique design standard that is established in the design cookbook.

Example

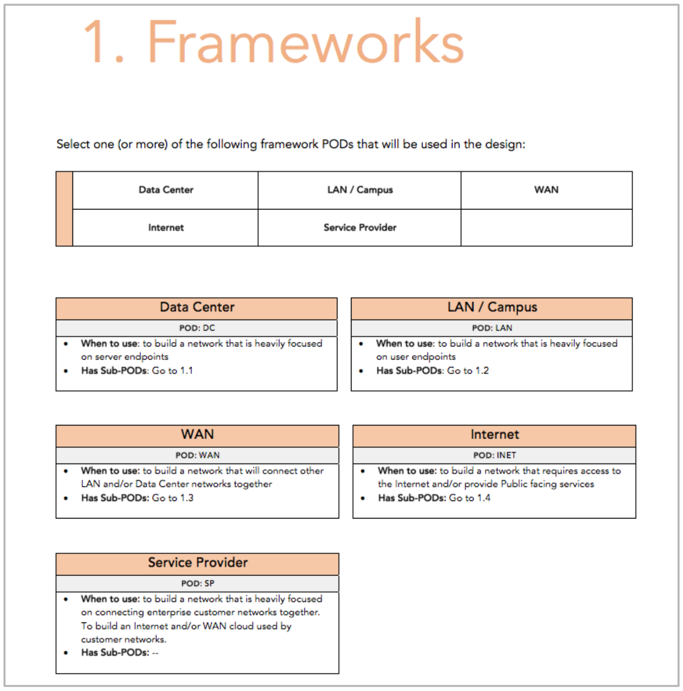
We will now go through a simple example that will bring everything together and show how to use the design cookbook to build your own design.

Here is a list of simple requirements and preferences that we will reference for this design:

- 100 Users
- Room: MDF (1) and Wiring Closet (1)
- Internet
- LAN
- Cloud Computing
- Wireless
- Hardware: Cisco (Switches, Routers), Fortinet (Firewall)
- No redundancy

(Step 1) Framework

First, we need to build the framework of our network. Therefore, we need to go to the "Framework" section:



1. Frameworks

Select one (or more) of the following framework PODs that will be used in the design:

	Data Center	**LAN / Campus**	**WAN**
	Internet	**Service Provider**	

Data Center

POD: DC

- **When to use**: to build a network that is heavily focused on server endpoints
- **Has Sub-PODs**: Go to 1.1

LAN / Campus

POD: LAN

- **When to use**: to build a network that is heavily focused on user endpoints
- **Has Sub-PODs**: Go to 1.2

WAN

POD: WAN

- **When to use:** to build a network that will connect other LAN and/or Data Center networks together
- **Has Sub-PODs:** Go to 1.3

Internet

POD: INET

- **When to use:** to build a network that requires access to the Internet and/or provide Public facing services
- **Has Sub-PODs:** Go to 1.4

Service Provider

POD: SP

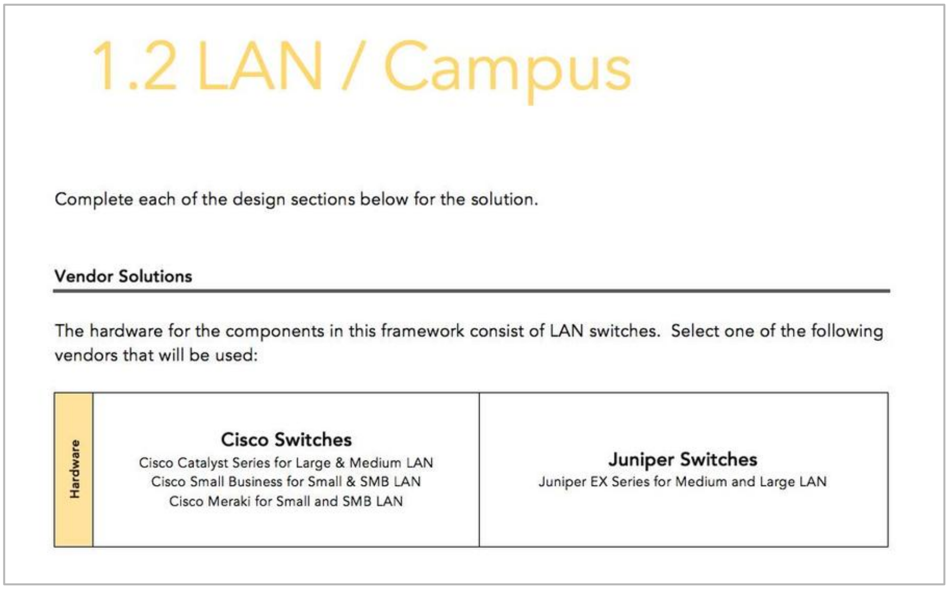
- **When to use:** to build a network that is heavily focused on connecting enterprise customer networks together. To build an Internet and/or WAN cloud used by customer networks.
- **Has Sub-PODs:** --

We need to select one (or more) of the following PODs. Here we would look at each POD and choose all that apply based on the business requirements and/or our preferences.

Looking at the available options, our network will heavily be focused on user endpoints and we do not have any remote sites. But we do require access to the Internet. Therefore, we will select the LAN and Internet PODs

- LAN POD
- Internet POD

Each of those has Sub-PODs available, so let's complete the LAN POD first before we do the Internet POD. Therefore, we need to go to section 1.2:



1.2 LAN / Campus

Complete each of the design sections below for the solution.

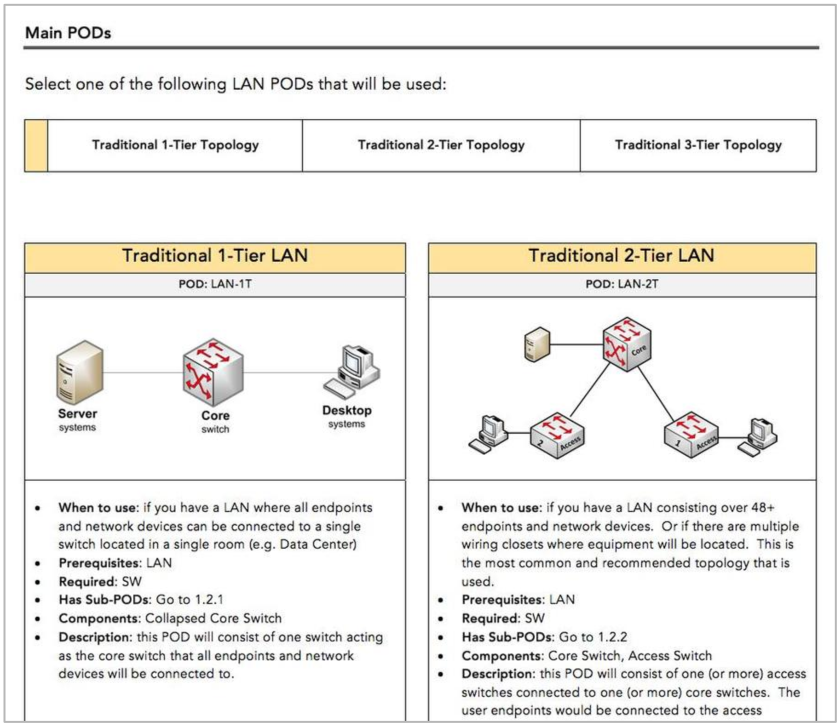
Vendor Solutions

The hardware for the components in this framework consist of LAN switches. Select one of the following vendors that will be used:

Hardware	**Cisco Switches** Cisco Catalyst Series for Large & Medium LAN Cisco Small Business for Small & SMB LAN Cisco Meraki for Small and SMB LAN	**Juniper Switches** Juniper EX Series for Medium and Large LAN

Once we go there, we need to first determine what vendor will be used for the network devices in the LAN POD. My experience is heavy with Cisco router and switches, so the primary vendor will be Cisco. This means using either Cisco Catalyst, Small Business, or Meraki Switches ideal for 100 user environments.

As we move down the page, we get to the main design PODs for the LAN.



Main PODs

Select one of the following LAN PODs that will be used:

🟨	**Traditional 1-Tier Topology**	**Traditional 2-Tier Topology**	**Traditional 3-Tier Topology**

Traditional 1-Tier LAN

POD: LAN-1T

- **When to use**: if you have a LAN where all endpoints and network devices can be connected to a single switch located in a single room (e.g. Data Center)
- **Prerequisites**: LAN
- **Required**: SW
- **Has Sub-PODs**: Go to 1.2.1
- **Components**: Collapsed Core Switch
- **Description**: this POD will consist of one switch acting as the core switch that all endpoints and network devices will be connected to.

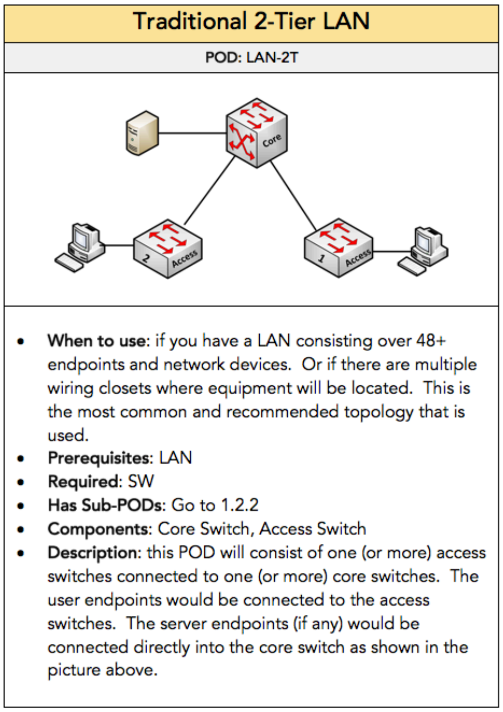
Traditional 2-Tier LAN

POD: LAN-2T

- **When to use**: if you have a LAN consisting over 48+ endpoints and network devices. Or if there are multiple wiring closets where equipment will be located. This is the most common and recommended topology that is used.
- **Prerequisites**: LAN
- **Required**: SW
- **Has Sub-PODs**: Go to 1.2.2
- **Components**: Core Switch, Access Switch
- **Description**: this POD will consist of one (or more) access switches connected to one (or more) core switches. The user endpoints would be connected to the access

This will show a summary POD reflecting three possible PODs we can choose from and we can only choose one of them. Again, we will look at each of the available PODs reading it's "When to use" design item.

We will select the Traditional 2-Tier LAN POD since it is the most common and that there will be multiple wiring closets with network devices.



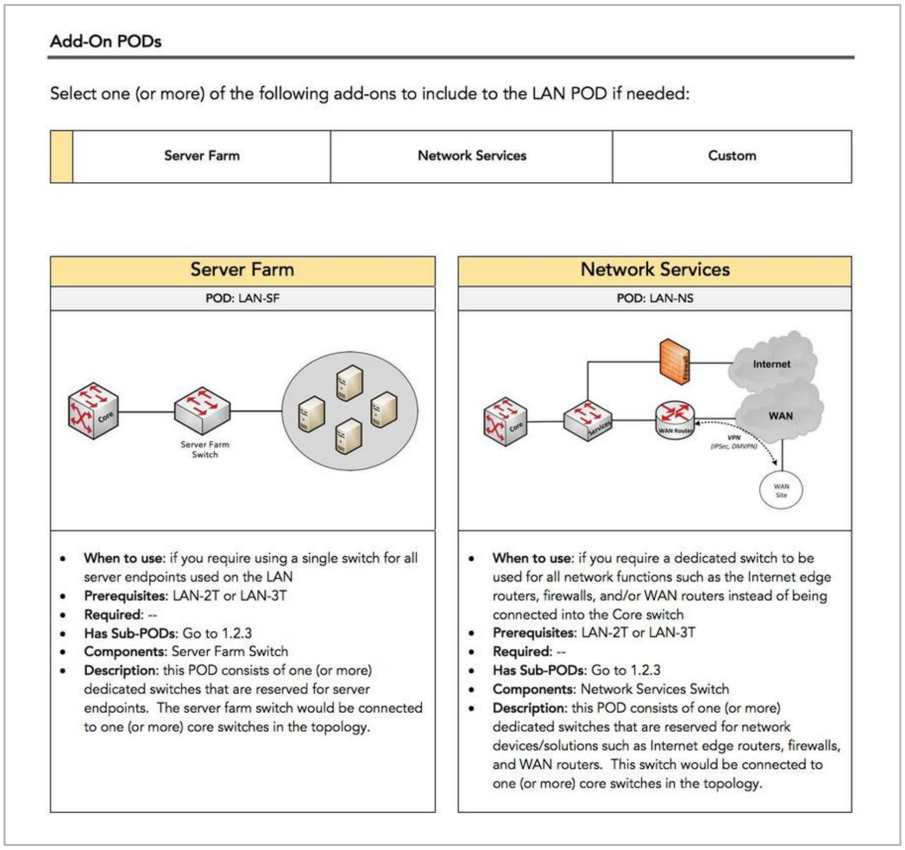
Traditional 2-Tier LAN

POD: LAN-2T

- **When to use**: if you have a LAN consisting over 48+ endpoints and network devices. Or if there are multiple wiring closets where equipment will be located. This is the most common and recommended topology that is used.
- **Prerequisites**: LAN
- **Required**: SW
- **Has Sub-PODs**: Go to 1.2.2
- **Components**: Core Switch, Access Switch
- **Description**: this POD will consist of one (or more) access switches connected to one (or more) core switches. The user endpoints would be connected to the access switches. The server endpoints (if any) would be connected directly into the core switch as shown in the picture above.

Choosing this POD, we see that we need to previously select the "LAN" POD which we already did. And we see that the "Switching" POD is required for this LAN topology.

Selecting that POD, there are additional PODs available. Before we do that, there are add-on PODs we could add this existing LAN POD:



Add-On PODs

Select one (or more) of the following add-ons to include to the LAN POD if needed:

Server Farm	Network Services	Custom

Server Farm

POD: LAN-SF

- **When to use**: if you require using a single switch for all server endpoints used on the LAN
- **Prerequisites**: LAN-2T or LAN-3T
- **Required**: --
- **Has Sub-PODs**: Go to 1.2.3
- **Components**: Server Farm Switch
- **Description**: this POD consists of one (or more) dedicated switches that are reserved for server endpoints. The server farm switch would be connected to one (or more) core switches in the topology.

Network Services

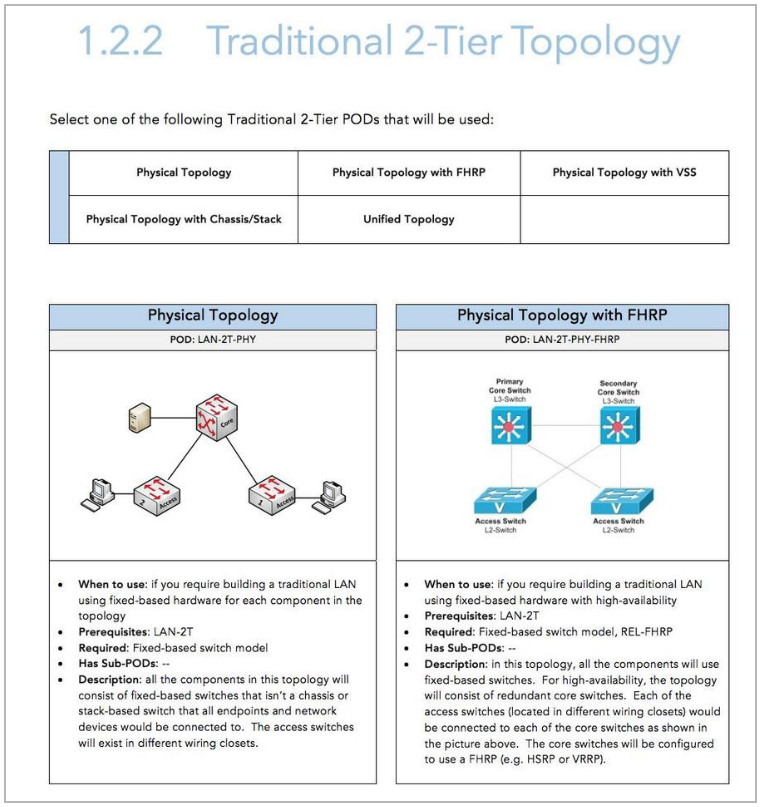
POD: LAN-NS

- **When to use**: if you require a dedicated switch to be used for all network functions such as the Internet edge routers, firewalls, and/or WAN routers instead of being connected into the Core switch
- **Prerequisites**: LAN-2T or LAN-3T
- **Required**: --
- **Has Sub-PODs**: Go to 1.2.3
- **Components**: Network Services Switch
- **Description**: this POD consists of one (or more) dedicated switches that are reserved for network devices/solutions such as Internet edge routers, firewalls, and WAN routers. This switch would be connected to one (or more) core switches in the topology.

Here we can select one (or more) of the following PODs. These are only applicable if you are using a 2-Tier LAN which is what we will use. But among these add-on PODs we do not require a dedicated switch for the server endpoints. There will be a few servers and they will be plugged directly into the Core switch. We also don't require a dedicated switch for our network solutions like a firewall or WAN router. We can plug those components into the Core switch. Furthermore, we don't have any requirements or need for a custom switch to provide a specific function. These decisions are based on my preferences and experiences. We don't need to add more hardware that isn't needed.

However, if you as the network architect want to use separate switches for network services or the server farm then you can easily include that to your design. That is another example that shows why each network design will be different and the available PODs listed shows the many possible ways how a network can be built.

Anyhow, since we don't have a need for any of these add-ons we can complete the design for the Tier-2 LAN, which has sub-PODs (section 1.2.2).



1.2.2 Traditional 2-Tier Topology

Select one of the following Traditional 2-Tier PODs that will be used:

Physical Topology	Physical Topology with FHRP	Physical Topology with VSS
Physical Topology with Chassis/Stack	Unified Topology	

Physical Topology

POD: LAN-2T-PHY

- **When to use**: if you require building a traditional LAN using fixed-based hardware for each component in the topology
- **Prerequisites**: LAN-2T
- **Required**: Fixed-based switch model
- **Has Sub-PODs**: --
- **Description**: all the components in this topology will consist of fixed-based switches that isn't a chassis or stack-based switch that all endpoints and network devices would be connected to. The access switches will exist in different wiring closets.

Physical Topology with FHRP

POD: LAN-2T-PHY-FHRP

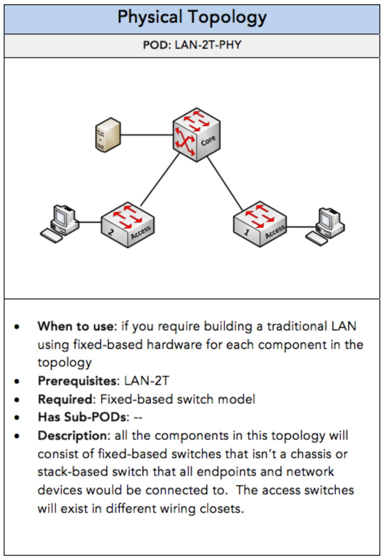
- **When to use**: if you require building a traditional LAN using fixed-based hardware with high-availability
- **Prerequisites**: LAN-2T
- **Required**: Fixed-based switch model, REL-FHRP
- **Has Sub-PODs**: --
- **Description**: in this topology, all the components will use fixed-based switches. For high-availability, the topology will consist of redundant core switches. Each of the access switches (located in different wiring closets) would be connected to each of the core switches as shown in the picture above. The core switches will be configured to use a FHRP (e.g. HSRP or VRRP).

This will show different ways how our Traditional 2-Tier LAN can be deployed. The summary POD shows 5 possible options and we need to select one of them.

Our network doesn't have any redundancy requirements, so that will eliminate half of these PODs such as "Physical Topology with FHRP", "Physical Topology with VSS" and "Physical Topology with Chassis/Stack".

The "Unified Topology" is not a specific preference of mine plus some of the equipment will exist in different rooms.

That will leave us with a Physical Traditional 2-Tier LAN Topology.



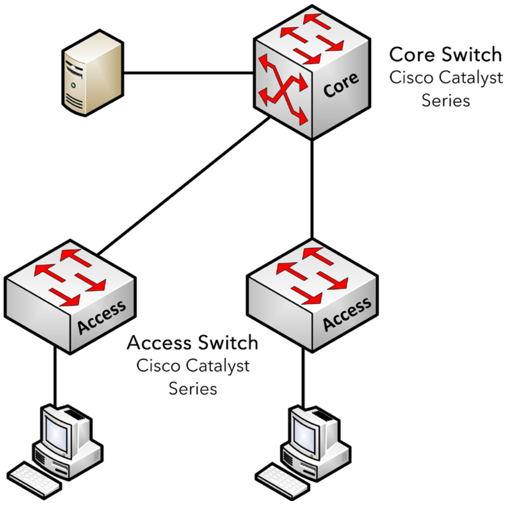
Physical Topology

POD: LAN-2T-PHY

Core
2 Access
1 Access

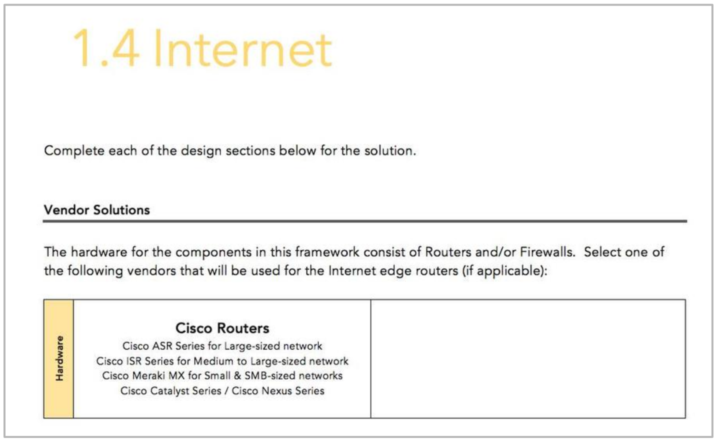
- **When to use**: if you require building a traditional LAN using fixed-based hardware for each component in the topology
- **Prerequisites**: LAN-2T
- **Required**: Fixed-based switch model
- **Has Sub-PODs**: --
- **Description**: all the components in this topology will consist of fixed-based switches that isn't a chassis or stack-based switch that all endpoints and network devices would be connected to. The access switches will exist in different wiring closets.

This will require fixed-based Cisco switches for each of the components in the LAN POD. Using a chassis-based switch or a stack-based switch is not required for our topology. Since there are no available Sub-PODs we are done with the LAN POD. Below reflects what our LAN in the topology will look like:



The number of access switches will depend on the port capacity and where they will located in the building.

Since the LAN is completed, we need to complete the Internet POD by going to section 1.4



1.4 Internet

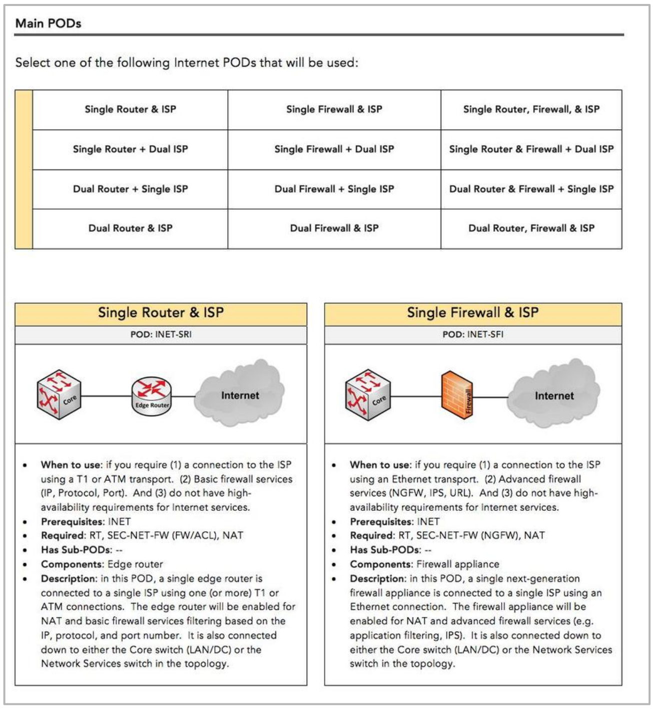
Complete each of the design sections below for the solution.

Vendor Solutions

The hardware for the components in this framework consist of Routers and/or Firewalls. Select one of the following vendors that will be used for the Internet edge routers (if applicable):

Hardware	**Cisco Routers** Cisco ASR Series for Large-sized network Cisco ISR Series for Medium to Large-sized network Cisco Meraki MX for Small & SMB-sized networks Cisco Catalyst Series / Cisco Nexus Series	

Again, just like the LAN POD, we need to determine the vendor that will be used.   This will only reflects router if our chosen POD will consist of a router component. For now, we will use Cisco for the router device and lets continue on until we get to the main PODs:



Main PODs

Select one of the following Internet PODs that will be used:

Single Router & ISP	Single Firewall & ISP	Single Router, Firewall, & ISP
Single Router + Dual ISP	Single Firewall + Dual ISP	Single Router & Firewall + Dual ISP
Dual Router + Single ISP	Dual Firewall + Single ISP	Dual Router & Firewall + Single ISP
Dual Router & ISP	Dual Firewall & ISP	Dual Router, Firewall & ISP

Single Router & ISP

POD: INET-SRI

- **When to use**: if you require (1) a connection to the ISP using a T1 or ATM transport. (2) Basic firewall services (IP, Protocol, Port). And (3) do not have high-availability requirements for Internet services.
- **Prerequisites**: INET
- **Required**: RT, SEC-NET-FW (FW/ACL), NAT
- **Has Sub-PODs**: --
- **Components**: Edge router
- **Description**: in this POD, a single edge router is connected to a single ISP using one (or more) T1 or ATM connections. The edge router will be enabled for NAT and basic firewall services filtering based on the IP, protocol, and port number. It is also connected down to either the Core switch (LAN/DC) or the Network Services switch in the topology.

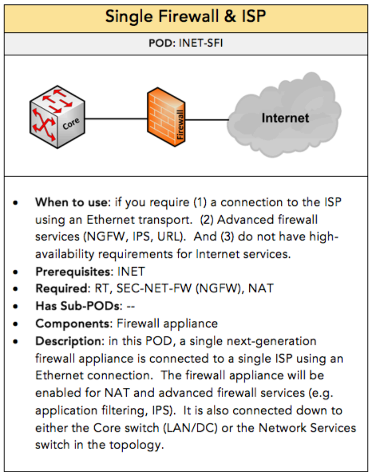
Single Firewall & ISP

POD: INET-SFI

- **When to use**: if you require (1) a connection to the ISP using an Ethernet transport. (2) Advanced firewall services (NGFW, IPS, URL). And (3) do not have high-availability requirements for Internet services.
- **Prerequisites**: INET
- **Required**: RT, SEC-NET-FW (NGFW), NAT
- **Has Sub-PODs**: --
- **Components**: Firewall appliance
- **Description**: in this POD, a single next-generation firewall appliance is connected to a single ISP using an Ethernet connection. The firewall appliance will be enabled for NAT and advanced firewall services (e.g. application filtering, IPS). It is also connected down to either the Core switch (LAN/DC) or the Network Services switch in the topology.

This will have several available PODs that we can choose from based on the summary POD. By looking at the name some will consist of a router or firewall or both. Some of these PODs consist of redundant routers, firewalls, and/or ISP. It is important to go through each POD to determine the best POD to use.

For us, we don't have any redundancy requirements and I want to consider a firewall appliance instead of a router device. Therefore, we will select the "Single Firewall & ISP" POD:



Single Firewall & ISP

POD: INET-SFI

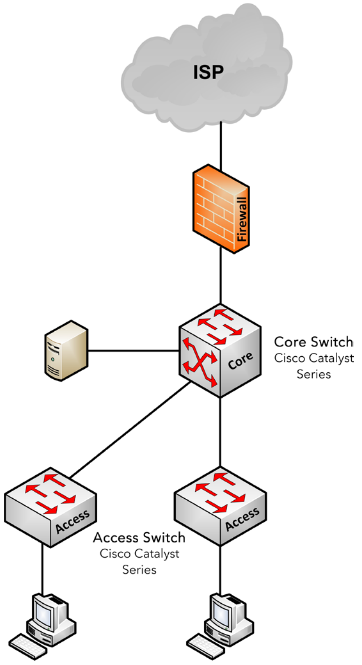
Core
Firewall
Internet

- **When to use**: if you require (1) a connection to the ISP using an Ethernet transport. (2) Advanced firewall services (NGFW, IPS, URL). And (3) do not have high-availability requirements for Internet services.
- **Prerequisites**: INET
- **Required**: RT, SEC-NET-FW (NGFW), NAT
- **Has Sub-PODs**: --
- **Components**: Firewall appliance
- **Description**: in this POD, a single next-generation firewall appliance is connected to a single ISP using an Ethernet connection. The firewall appliance will be enabled for NAT and advanced firewall services (e.g. application filtering, IPS). It is also connected down to either the Core switch (LAN/DC) or the Network Services switch in the topology.

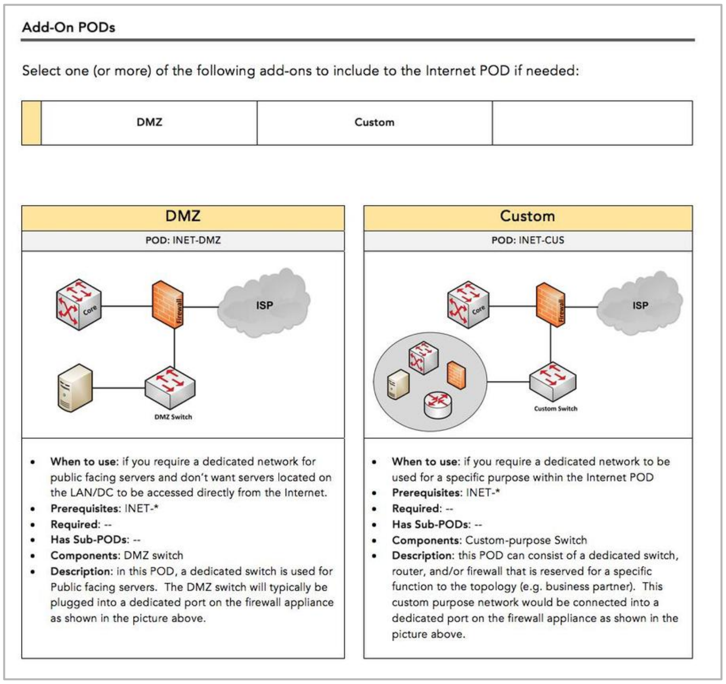
The prerequisite to use this POD is the "INET" POD which is what we determined initially. But we see some requirements that must be added:

- Routing POD (POD ID: RT)
- NGFW appliance (POD ID: SEC-NET-FW)
- NAT POD (POD ID: NAT)

There are no additional Sub-PODs to choose from, therefore, the following diagram would be our Internet topology and how it would be connected into the LAN Core which was mentioned in the description:



The Internet POD also has some add-on PODs for including a DMZ or a custom network:



Add-On PODs

Select one (or more) of the following add-ons to include to the Internet POD if needed:

	DMZ	Custom	

DMZ

POD: INET-DMZ

- **When to use**: if you require a dedicated network for public facing servers and don't want servers located on the LAN/DC to be accessed directly from the Internet.
- **Prerequisites**: INET-*
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: DMZ switch
- **Description**: in this POD, a dedicated switch is used for Public facing servers. The DMZ switch will typically be plugged into a dedicated port on the firewall appliance as shown in the picture above.

Custom

POD: INET-CUS

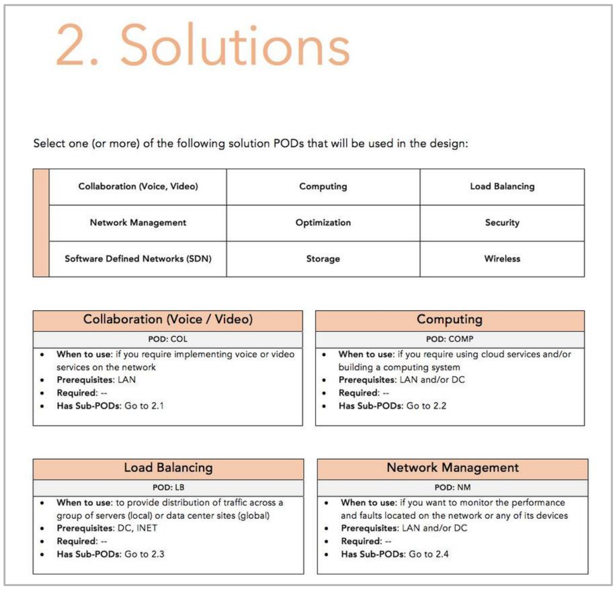
- **When to use**: if you require a dedicated network to be used for a specific purpose within the Internet POD
- **Prerequisites**: INET-*
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Custom-purpose Switch
- **Description**: this POD can consist of a dedicated switch, router, and/or firewall that is reserved for a specific function to the topology (e.g. business partner). This custom purpose network would be connected into a dedicated port on the firewall appliance as shown in the picture above.

In our environment, we do not have any unique requirements for these additions to the Internet POD.

At this time, we are finished with the Framework.

(Step 2) Solutions

Now we can determine what solutions should be added on-top of our Internet and LAN topology. This means we need to go to section 2 to see our available options:



2. Solutions

Select one (or more) of the following solution PODs that will be used in the design:

Collaboration (Voice, Video)	Computing	Load Balancing
Network Management	Optimization	Security
Software Defined Networks (SDN)	Storage	Wireless

Collaboration (Voice / Video)

POD: COL

- **When to use:** if you require implementing voice or video services on the network
- **Prerequisites:** LAN
- **Required:** --
- **Has Sub-PODs:** Go to 2.1

Computing

POD: COMP

- **When to use:** if you require using cloud services and/or building a computing system
- **Prerequisites:** LAN and/or DC
- **Required:** --
- **Has Sub-PODs:** Go to 2.2

Load Balancing

POD: LB

- **When to use:** to provide distribution of traffic across a group of servers (local) or data center sites (global)
- **Prerequisites:** DC, INET
- **Required:** --
- **Has Sub-PODs:** Go to 2.3

Network Management

POD: NM

- **When to use:** if you want to monitor the performance and faults located on the network or any of its devices
- **Prerequisites:** LAN and/or DC
- **Required:** --
- **Has Sub-PODs:** Go to 2.4

There are a lot of possible solutions that can be deployed and we can review each of these PODs to determine which ones are required. For our example, based on the business requirements we know that the environment will be using cloud computing services on the Internet. And they will require Wireless capabilities since most of the employees will have laptops. This means the following solutions PODs will be chosen:

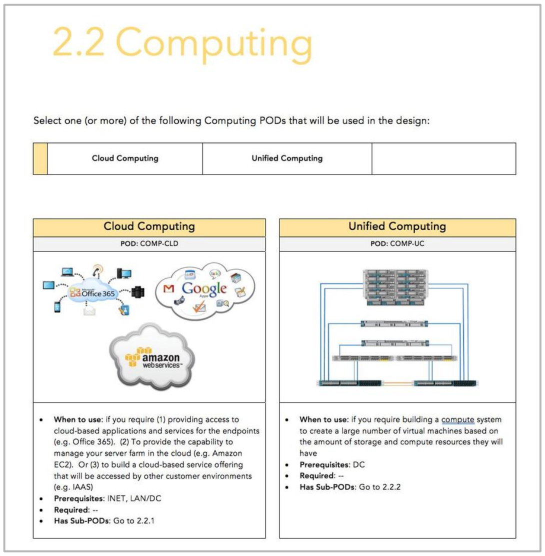
- Computing
- Wireless

As the engineer we can recommend other solutions that the business won't necessarily know they need such as network security or network monitoring. This is the value we bring to the customer as the network architect/engineer. Therefore, we will include the following solution PODs to the design:

- Security
- Network Management

Looking at each of the solution PODs that our design will use, we need to look at its prerequisites. For most of these solutions we must have a LAN or DC including an Internet POD. For us, we already completed the design for the LAN and Internet topology.

From here, we will need to go through each POD and complete the design for that solution. I will show some of these solution in this example. We will begin with the "Computing" POD which is one of the business requirements. This has a prerequisite for the LAN POD which we already completed. We also see there are sub-PODs available so we need to go to section 2.2


Office 365
Google
amazon web services

2.2 Computing

Select one (or more) of the following Computing PODs that will be used in the design:

	Cloud Computing	Unified Computing	

Cloud Computing

POD: COMP-CLD

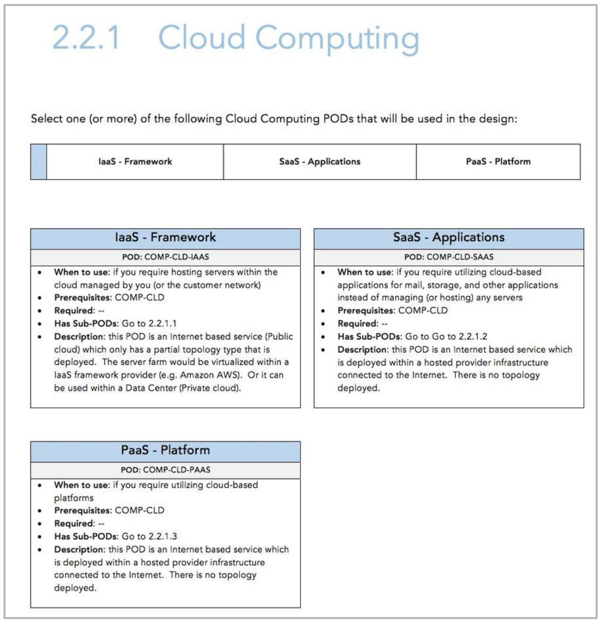
- **When to use:** if you require (1) providing access to cloud-based applications and services for the endpoints (e.g. Office 365). (2) To provide the capability to manage your server farm in the cloud (e.g. Amazon EC2). Or (3) to build a cloud-based service offering that will be accessed by other customer environments (e.g. IAAS)
- **Prerequisites**: INET, LAN/DC
- **Required**: --
- **Has Sub-PODs**: Go to 2.2.1

Unified Computing

POD: COMP-UC

- **When to use:** if you require building a compute system to create a large number of virtual machines based on the amount of storage and compute resources they will have
- **Prerequisites**: DC
- **Required**: --
- **Has Sub-PODs**: Go to 2.2.2

There are two type of computing solutions. There is cloud computing and unified computing. We need to select all computing PODs that are required in our environment and that will be the "Cloud Computing" POD. This has a prerequisite for a LAN and Internet POD. Plus there are sub-PODs available which means we need to go to section 2.2.1.



2.2.1 Cloud Computing

Select one (or more) of the following Cloud Computing PODs that will be used in the design:

	IaaS - Framework	SaaS - Applications	PaaS - Platform

IaaS - Framework

POD: COMP-CLD-IAAS

- **When to use**: if you require hosting servers within the cloud managed by you (or the customer network)
- **Prerequisites**: COMP-CLD
- **Required**: --
- **Has Sub-PODs**: Go to 2.2.1.1
- **Description**: this POD is an Internet based service (Public cloud) which only has a partial topology type that is deployed. The server farm would be virtualized within a IaaS framework provider (e.g. Amazon AWS). Or it can be used within a Data Center (Private cloud).

SaaS - Applications

POD: COMP-CLD-SAAS

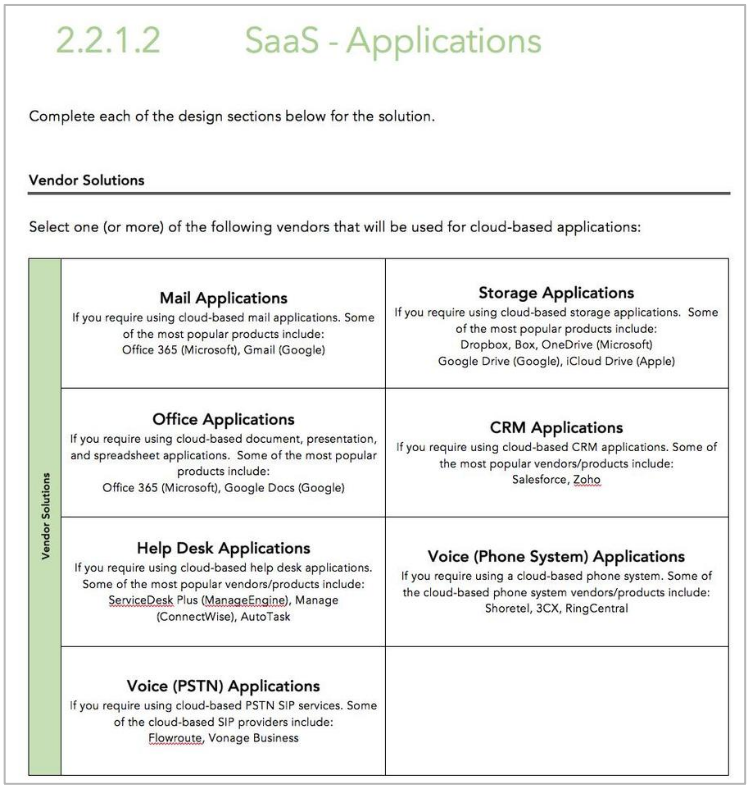
- **When to use**: if you require utilizing cloud-based applications for mail, storage, and other applications instead of managing (or hosting) any servers
- **Prerequisites**: COMP-CLD
- **Required**: --
- **Has Sub-PODs**: Go to Go to 2.2.1.2
- **Description**: this POD is an Internet based service which is deployed within a hosted provider infrastructure connected to the Internet. There is no topology deployed.

PaaS - Platform

POD: COMP-CLD-PAAS

- **When to use**: if you require utilizing cloud-based platforms
- **Prerequisites**: COMP-CLD
- **Required**: --
- **Has Sub-PODs**: Go to 2.2.1.3
- **Description**: this POD is an Internet based service which is deployed within a hosted provider infrastructure connected to the Internet. There is no topology deployed.

Next, we need to select one or more of the following "cloud computing" PODs that will be used. Again, we need to review all of the design items such as "When to use", the description, and if any sub-PODs are available to complete this design POD. Among the available PODs here, we will only select the "SaaS" POD since the business will be using computing services such as Office 365 and Dropbox. Thus, we need to continue on to section 2.2.1.2.



2.2.1.2 SaaS - Applications

Complete each of the design sections below for the solution.

Vendor Solutions

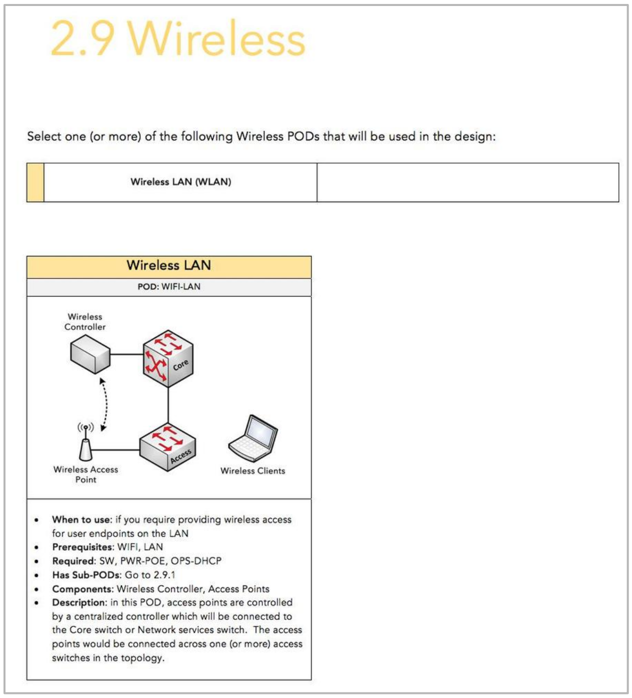
Select one (or more) of the following vendors that will be used for cloud-based applications:

Vendor Solutions	**Mail Applications** If you require using cloud-based mail applications. Some of the most popular products include: Office 365 (Microsoft), Gmail (Google)	**Storage Applications** If you require using cloud-based storage applications. Some of the most popular products include: Dropbox, Box, OneDrive (Microsoft) Google Drive (Google), iCloud Drive (Apple)
	Office Applications If you require using cloud-based document, presentation, and spreadsheet applications. Some of the most popular products include: Office 365 (Microsoft), Google Docs (Google)	**CRM Applications** If you require using cloud-based CRM applications. Some of the most popular vendors/products include: Salesforce, Zoho
	Help Desk Applications If you require using cloud-based help desk applications. Some of the most popular vendors/products include: ServiceDesk Plus (ManageEngine), Manage (ConnectWise), AutoTask	**Voice (Phone System) Applications** If you require using a cloud-based phone system. Some of the cloud-based phone system vendors/products include: Shoretel, 3CX, RingCentral
	Voice (PSTN) Applications If you require using cloud-based PSTN SIP services. Some of the cloud-based SIP providers include: Flowroute, Vonage Business	

And this will show Grid PODs reflecting some of the main SaaS categories followed by products that can be considered unless the business specifically ask for it. For our example, the customer will be using Office 365 (Mail & Office Applications) and Dropbox (Storage Applications).

At this stage, we are done with the "Computing" POD.

Moving on to the "Wireless" POD which has a prerequisite of a LAN POD, we will proceed to section to 2.9:



2.9 Wireless

Select one (or more) of the following Wireless PODs that will be used in the design:

	Wireless LAN (WLAN)	

Wireless LAN

POD: WIFI-LAN

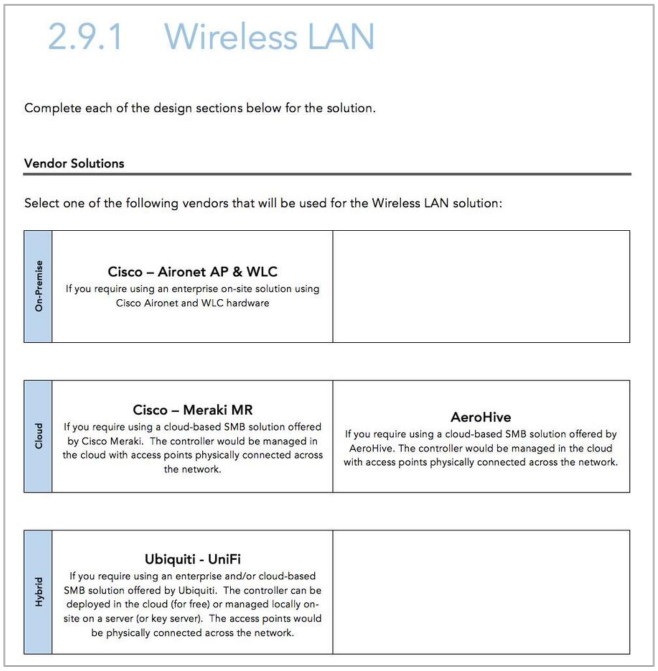
- **When to use:** if you require providing wireless access for user endpoints on the LAN
- **Prerequisites:** WIFI, LAN
- **Required:** SW, PWR-POE, OPS-DHCP
- **Has Sub-PODs:** Go to 2.9.1
- **Components:** Wireless Controller, Access Points
- **Description:** in this POD, access points are controlled by a centralized controller which will be connected to the Core switch or Network services switch. The access points would be connected across one (or more) access switches in the topology.

This will reflect the different types of "Wireless" PODs we may build, but we will select the "Wireless LAN" POD which is currently the only POD listed in the design cookbook. This has a requirement for the following PODs:

- Switching
- POE
- DHCP

The Switching POD was previously added to our design list when we completed the LAN POD.

Next, within the POD details we will continue on to section 2.9.1



2.9.1 Wireless LAN

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for the Wireless LAN solution:

On-Premise	**Cisco – Aironet AP & WLC** If you require using an enterprise on-site solution using Cisco Aironet and WLC hardware	

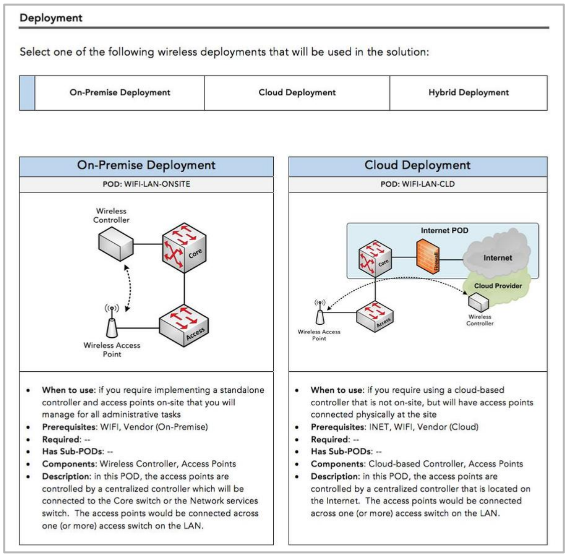
Cloud	**Cisco – Meraki MR** If you require using a cloud-based SMB solution offered by Cisco Meraki. The controller would be managed in the cloud with access points physically connected across the network.	**AeroHive** If you require using a cloud-based SMB solution offered by AeroHive. The controller would be managed in the cloud with access points physically connected across the network.

Hybrid	**Ubiquiti - UniFi** If you require using an enterprise and/or cloud-based SMB solution offered by Ubiquiti. The controller can be deployed in the cloud (for free) or managed locally on-site on a server (or key server). The access points would be physically connected across the network.	

Here we need to determine what Wireless vendor we want to consider for this solution. As the network architect, we can choose one of the listed vendor solutions (or not listed) based on our preferences if it meets the business requirements.

These are Grid PODs and they are grouped together based on the type which can be an on-premise solution, a cloud solution, or a hybrid between the two. For our decision, we will select UniFi (Ubiquiti) for the vendor solution which has been a favorite of mine for years.

Next we will move down the page and get to the deployment PODs section. This will show all of the possible ways the "Wireless" POD can be deployed in the environment based on the selected vendor solution.



Deployment

Select one of the following wireless deployments that will be used in the solution:

On-Premise Deployment	Cloud Deployment	Hybrid Deployment

On-Premise Deployment

POD: WIFI-LAN-ONSITE

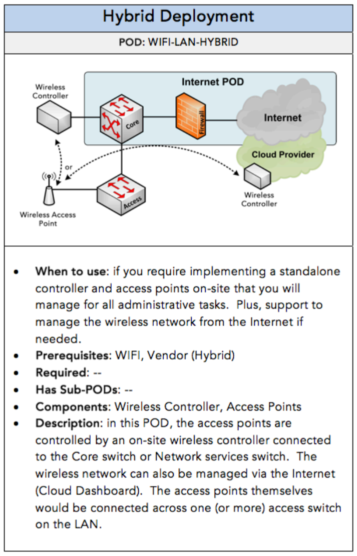
- **When to use:** if you require implementing a standalone controller and access points on-site that you will manage for all administrative tasks
- **Prerequisites:** WIFI, Vendor (On-Premise)
- **Required:** --
- **Has Sub-PODs:** --
- **Components:** Wireless Controller, Access Points
- **Description:** in this POD, the access points are controlled by a centralized controller which will be connected to the Core switch or the Network services switch. The access points would be connected across one (or more) access switch on the LAN.

Cloud Deployment

POD: WIFI-LAN-CLD

- **When to use:** if you require using a cloud-based controller that is not on-site, but will have access points connected physically at the site
- **Prerequisites:** INET, WIFI, Vendor (Cloud)
- **Required:** --
- **Has Sub-PODs:** --
- **Components:** Cloud-based Controller, Access Points
- **Description:** in this POD, the access points are controlled by a centralized controller that is located on the Internet. The access points would be connected across one (or more) access switch on the LAN.

For us, we selected UniFi (Ubiquiti) which is a Hybrid vendor solution. Therefore, we will use the Hybrid Deployment which will show how the solution will be deployed in the existing environment.



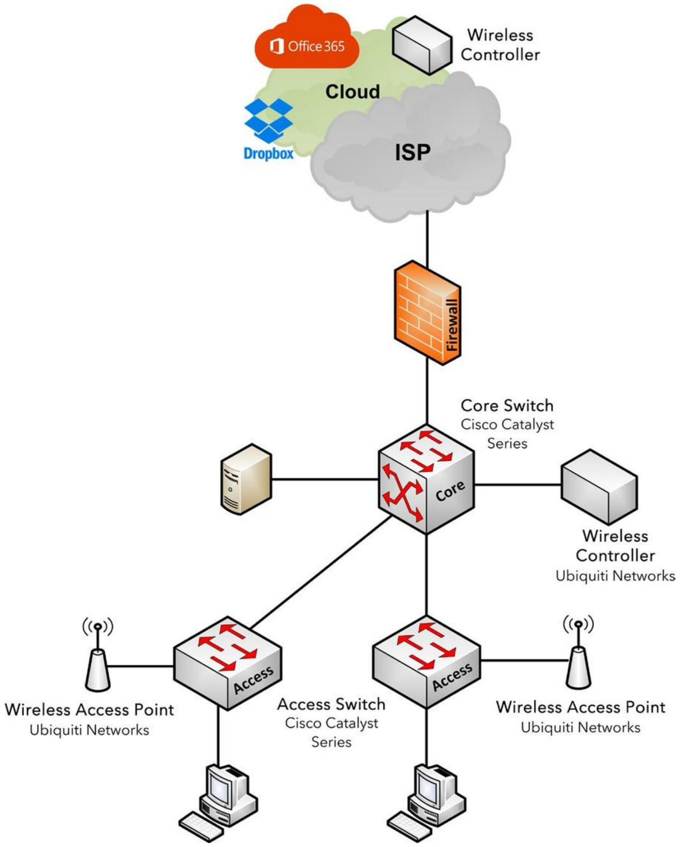
Hybrid Deployment

POD: WIFI-LAN-HYBRID

- **When to use**: if you require implementing a standalone controller and access points on-site that you will manage for all administrative tasks. Plus, support to manage the wireless network from the Internet if needed.
- **Prerequisites**: WIFI, Vendor (Hybrid)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Wireless Controller, Access Points
- **Description**: in this POD, the access points are controlled by an on-site wireless controller connected to the Core switch or Network services switch. The wireless network can also be managed via the Internet (Cloud Dashboard). The access points themselves would be connected across one (or more) access switch on the LAN.

The design picture shows the main wireless components based on the vendor solution and where they should connected on the LAN. This is why the LAN POD was a prerequisite for the "Wireless" POD because we needed the topology to already exist. The description listed for that POD will also explain the same thing.

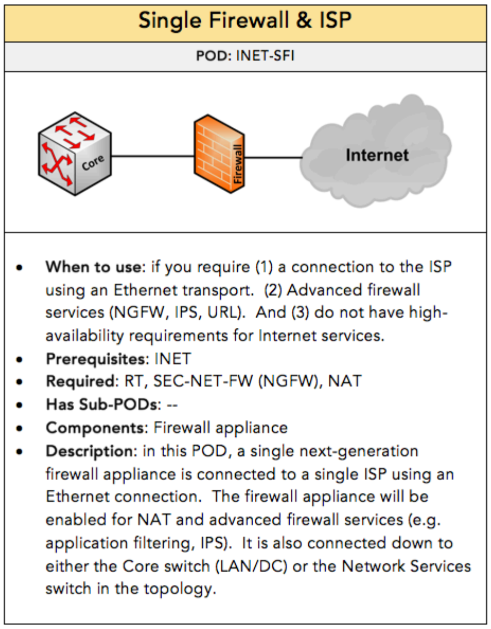
At this point, we are done with all of the solutions based on the business requirements. Here is an update to our existing design which now includes the "Wireless" POD:



We can continue the same process for the other solutions that we, as the network architect/engineer, recommended.

We won't do the "Network Management" POD, but let’s do the "Security" POD mostly because we need to anyway based on the "Internet" POD that we will use.

If you remember, the "Internet" POD will consist of a single firewall and ISP:

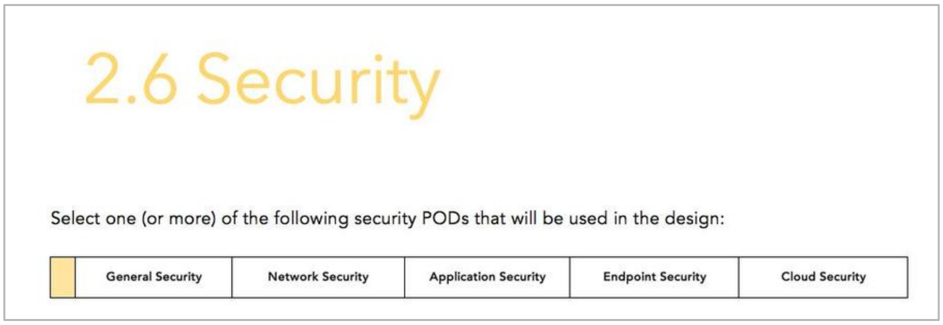


Single Firewall & ISP

POD: INET-SFI

- **When to use:** if you require (1) a connection to the ISP using an Ethernet transport. (2) Advanced firewall services (NGFW, IPS, URL). And (3) do not have high-availability requirements for Internet services.
- **Prerequisites**: INET
- **Required**: RT, SEC-NET-FW (NGFW), NAT
- **Has Sub-PODs**: --
- **Components**: Firewall appliance
- **Description**: in this POD, a single next-generation firewall appliance is connected to a single ISP using an Ethernet connection. The firewall appliance will be enabled for NAT and advanced firewall services (e.g. application filtering, IPS). It is also connected down to either the Core switch (LAN/DC) or the Network Services switch in the topology.

This requires the SEC-NET-FW POD and using a NGFW appliance which will be used within that POD. Looking at the POD ID, it starts with SEC which is the prefix for the "Security" POD that we recommended for this customer design. Therefore, let’s go to section 2.6 to build parts of the "Security" POD



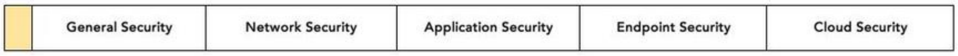
2.6 Security

Select one (or more) of the following security PODs that will be used in the design:

🟨	General Security	Network Security	Application Security	Endpoint Security	Cloud Security

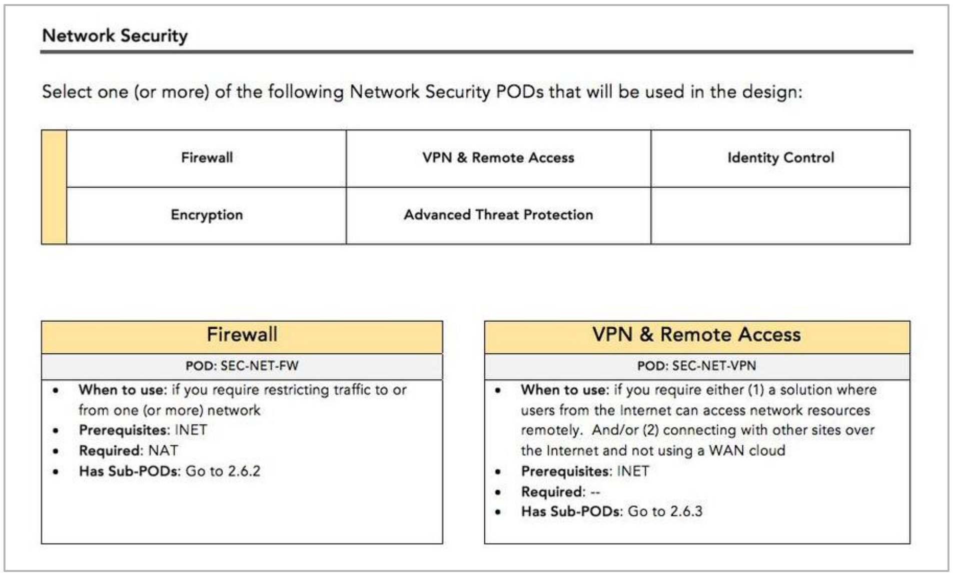
The "Security" POD is by far the largest section in the design cookbook providing security practices not only on the network but with applications and the endpoints. Threats are evolving, as a result, so does IT security. In the first part of this POD, it will outline the different types and layers to security. It is important to read through the information presented here to understand how to build end-to-end security.

You will also see a summary POD reflecting the major categories for security:



General Security	Network Security	Application Security	Endpoint Security	Cloud Security

These major categories are broken up further, but among them we will focus on Network Security. As you scroll down the page you will reach the Network Security section which will list its own summary and basic PODs:



Network Security

Select one (or more) of the following Network Security PODs that will be used in the design:

Firewall	VPN & Remote Access	Identity Control
Encryption	Advanced Threat Protection	

Firewall

POD: SEC-NET-FW

- **When to use:** if you require restricting traffic to or from one (or more) network
- **Prerequisites:** INET
- **Required:** NAT
- **Has Sub-PODs:** Go to 2.6.2

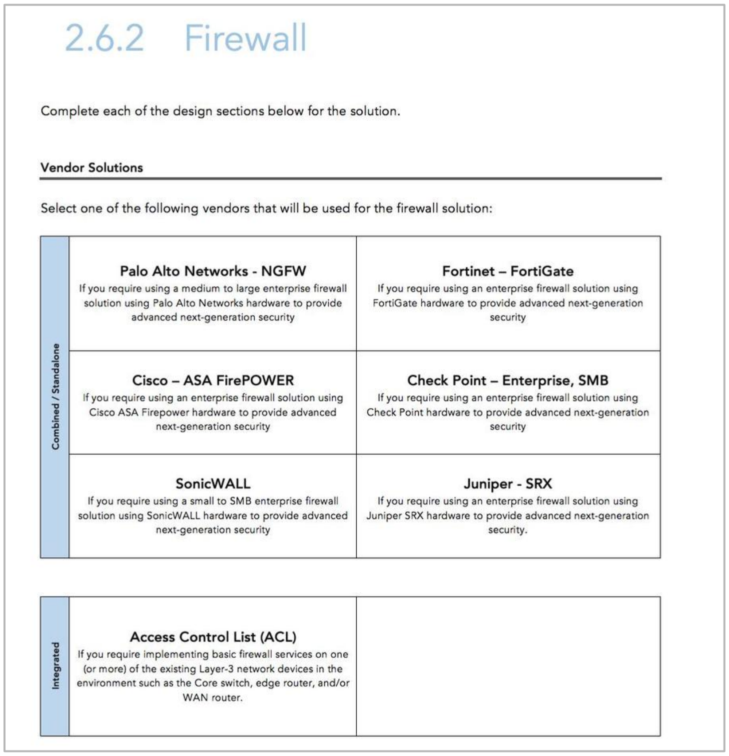
VPN & Remote Access

POD: SEC-NET-VPN

- **When to use:** if you require either (1) a solution where users from the Internet can access network resources remotely. And/or (2) connecting with other sites over the Internet and not using a WAN cloud
- **Prerequisites:** INET
- **Required:** --
- **Has Sub-PODs:** Go to 2.6.3

Among these PODs, we will select only the firewall POD since that is required for this customer design. Looking at the POD details we need to have an Internet POD completed and it requires a NAT POD with our design.

We need to go to section 2.6.2 to build out our firewall which exist inside of the Internet POD:



2.6.2 Firewall

Complete each of the design sections below for the solution.

Vendor Solutions

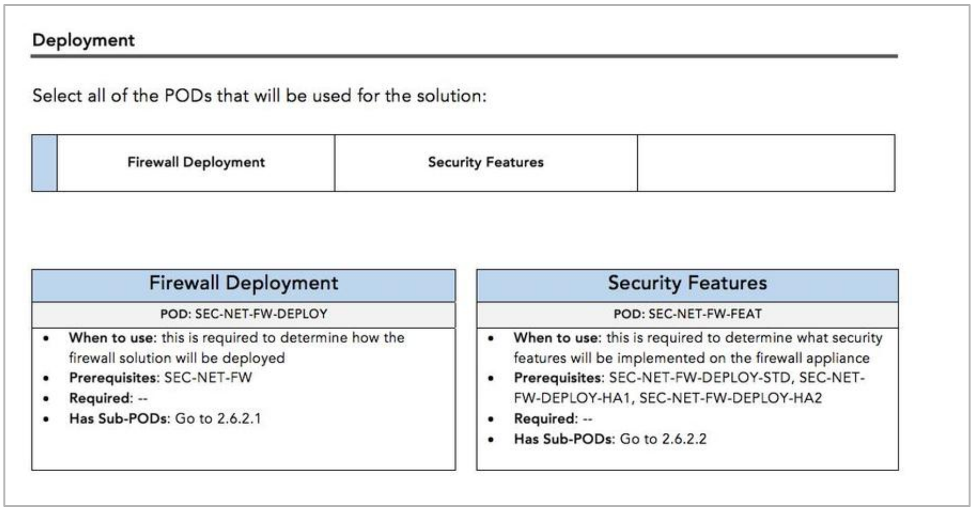
Select one of the following vendors that will be used for the firewall solution:

Combined / Standalone	**Palo Alto Networks - NGFW** If you require using a medium to large enterprise firewall solution using Palo Alto Networks hardware to provide advanced next-generation security	**Fortinet – FortiGate** If you require using an enterprise firewall solution using FortiGate hardware to provide advanced next-generation security
	Cisco – ASA FirePOWER If you require using an enterprise firewall solution using Cisco ASA Firepower hardware to provide advanced next-generation security	**Check Point – Enterprise, SMB** If you require using an enterprise firewall solution using Check Point hardware to provide advanced next-generation security
	SonicWALL If you require using a small to SMB enterprise firewall solution using SonicWALL hardware to provide advanced next-generation security	**Juniper - SRX** If you require using an enterprise firewall solution using Juniper SRX hardware to provide advanced next-generation security.

Integrated	**Access Control List (ACL)** If you require implementing basic firewall services on one (or more) of the existing Layer-3 network devices in the environment such as the Core switch, edge router, and/or WAN router.	

Just like the other solutions we completed so far we first need to determine the firewall vendor that will be used. I have a strong preference for Fortinet's FortiGate NGFW so that will be selected for this customer design.

As we continue on with our firewall design we need to complete each of the listed deployment PODs that are shown.



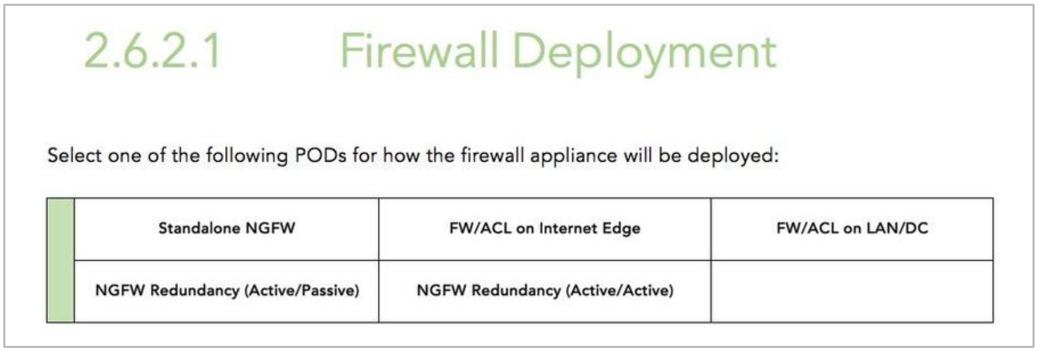
Deployment

Select all of the PODs that will be used for the solution:

🟦	Firewall Deployment	Security Features	

Firewall Deployment	Security Features
POD: SEC-NET-FW-DEPLOY	POD: SEC-NET-FW-FEAT
• **When to use:** this is required to determine how the firewall solution will be deployed • **Prerequisites:** SEC-NET-FW • **Required:** -- • **Has Sub-PODs:** Go to 2.6.2.1	• **When to use:** this is required to determine what security features will be implemented on the firewall appliance • **Prerequisites:** SEC-NET-FW-DEPLOY-STD, SEC-NET-FW-DEPLOY-HA1, SEC-NET-FW-DEPLOY-HA2 • **Required:** -- • **Has Sub-PODs:** Go to 2.6.2.2

We will start with the Firewall Deployment POD since that doesn't have any extra prerequisites compared to what we see under "Security Features". We need to go to section 2.6.2.1



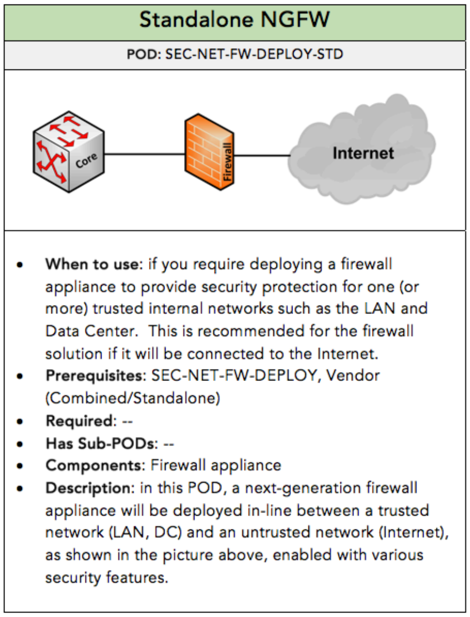
2.6.2.1 Firewall Deployment

Select one of the following PODs for how the firewall appliance will be deployed:

🟩	Standalone NGFW	FW/ACL on Internet Edge	FW/ACL on LAN/DC
	NGFW Redundancy (Active/Passive)	NGFW Redundancy (Active/Active)	

Here, we need to select one of the following PODs that will be used for our firewall deployment within the Internet POD. Again, we know there are no requirements for redundancy. This will eliminate the two NGFW Redundancy PODs that we see listed here. The FW/ACL PODs only apply if we want to implement firewall restrictions on the VLANs within the LAN/DC. Or on the edge router, but our design is using a dedicated firewall appliance.

Therefore, we will be using a standalone NGFW deployment.

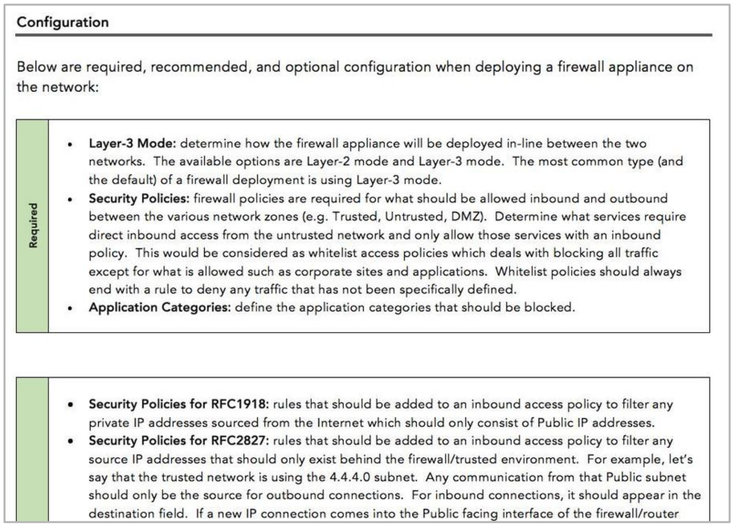


Standalone NGFW

POD: SEC-NET-FW-DEPLOY-STD

- **When to use**: if you require deploying a firewall appliance to provide security protection for one (or more) trusted internal networks such as the LAN and Data Center. This is recommended for the firewall solution if it will be connected to the Internet.
- **Prerequisites**: SEC-NET-FW-DEPLOY, Vendor (Combined/Standalone)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Firewall appliance
- **Description**: in this POD, a next-generation firewall appliance will be deployed in-line between a trusted network (LAN, DC) and an untrusted network (Internet), as shown in the picture above, enabled with various security features.

Doing this will not change the overall look of our design in the Internet POD. As we move down the page, there is a Configuration section with Required, Recommended, and Optional PODs which we covered before.



Configuration

Below are required, recommended, and optional configuration when deploying a firewall appliance on the network:

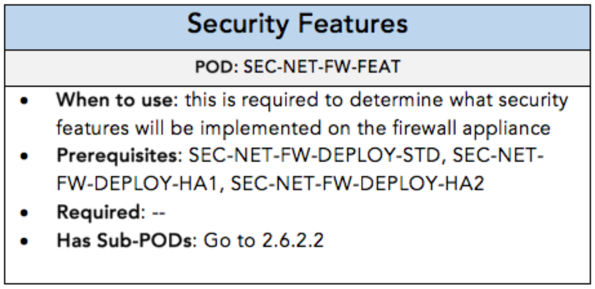
Required

- **Layer-3 Mode:** determine how the firewall appliance will be deployed in-line between the two networks. The available options are Layer-2 mode and Layer-3 mode. The most common type (and the default) of a firewall deployment is using Layer-3 mode.
- **Security Policies:** firewall policies are required for what should be allowed inbound and outbound between the various network zones (e.g. Trusted, Untrusted, DMZ). Determine what services require direct inbound access from the untrusted network and only allow those services with an inbound policy. This would be considered as whitelist access policies which deals with blocking all traffic except for what is allowed such as corporate sites and applications. Whitelist policies should always end with a rule to deny any traffic that has not been specifically defined.
- **Application Categories:** define the application categories that should be blocked.

- **Security Policies for RFC1918:** rules that should be added to an inbound access policy to filter any private IP addresses sourced from the Internet which should only consist of Public IP addresses.
- **Security Policies for RFC2827:** rules that should be added to an inbound access policy to filter any source IP addresses that should only exist behind the firewall/trusted environment. For example, let's say that the trusted network is using the 4.4.4.0 subnet. Any communication from that Public subnet should only be the source for outbound connections. For inbound connections, it should appear in the destination field. If a new IP connection comes into the Public facing interface of the firewall/router

These will simply list what we need to configure on that firewall appliance along with any other recommended configuration. This can be extremely helpful to us and the network engineers who will deploy this appliance on the network.

We are done with the firewall deployment POD, so now we need to complete the security features POD that we saw earlier:

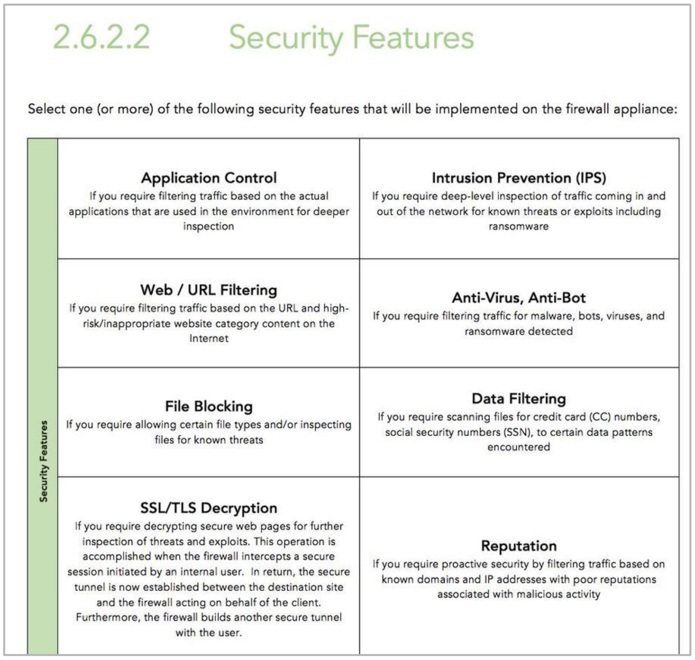


Security Features

POD: SEC-NET-FW-FEAT

- **When to use**: this is required to determine what security features will be implemented on the firewall appliance
- **Prerequisites**: SEC-NET-FW-DEPLOY-STD, SEC-NET-FW-DEPLOY-HA1, SEC-NET-FW-DEPLOY-HA2
- **Required**: --
- **Has Sub-PODs**: Go to 2.6.2.2

Moving forward with this POD has some prerequisites and one of the POD IDs listed is what we choose SEC-NET-FW-DEPLOY-STD (Standalone NGFW). Therefore, we can proceed on to its sub-PODs in section 2.6.2.2



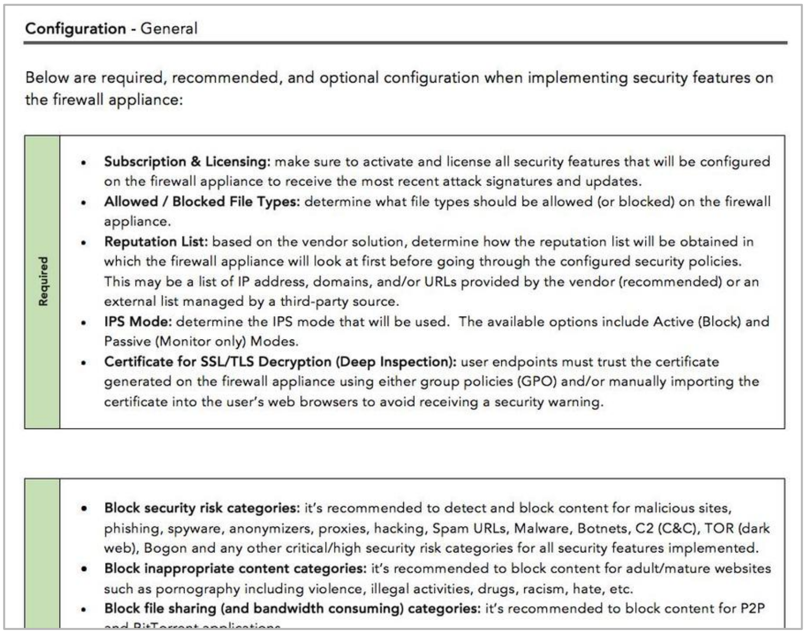
2.6.2.2 Security Features

Select one (or more) of the following security features that will be implemented on the firewall appliance:

Security Features	**Application Control** If you require filtering traffic based on the actual applications that are used in the environment for deeper inspection	**Intrusion Prevention (IPS)** If you require deep-level inspection of traffic coming in and out of the network for known threats or exploits including ransomware
	Web / URL Filtering If you require filtering traffic based on the URL and high-risk/inappropriate website category content on the Internet	**Anti-Virus, Anti-Bot** If you require filtering traffic for malware, bots, viruses, and ransomware detected
	File Blocking If you require allowing certain file types and/or inspecting files for known threats	**Data Filtering** If you require scanning files for credit card (CC) numbers, social security numbers (SSN), to certain data patterns encountered
	SSL/TLS Decryption If you require decrypting secure web pages for further inspection of threats and exploits. This operation is accomplished when the firewall intercepts a secure session initiated by an internal user. In return, the secure tunnel is now established between the destination site and the firewall acting on behalf of the client. Furthermore, the firewall builds another secure tunnel with the user.	**Reputation** If you require proactive security by filtering traffic based on known domains and IP addresses with poor reputations associated with malicious activity

This will simply list Grid PODs with a list of security features that can be implemented on the firewall appliance if it is supported. This can also provide a good list that we can follow for what security enhancements we can enable. Or knowing what type of NGFW features are available. There are new security features being released all the time and those additions can easily be added here in this section.

This POD has other parts such as the Configuration POD:



Configuration - General

Below are required, recommended, and optional configuration when implementing security features on the firewall appliance:

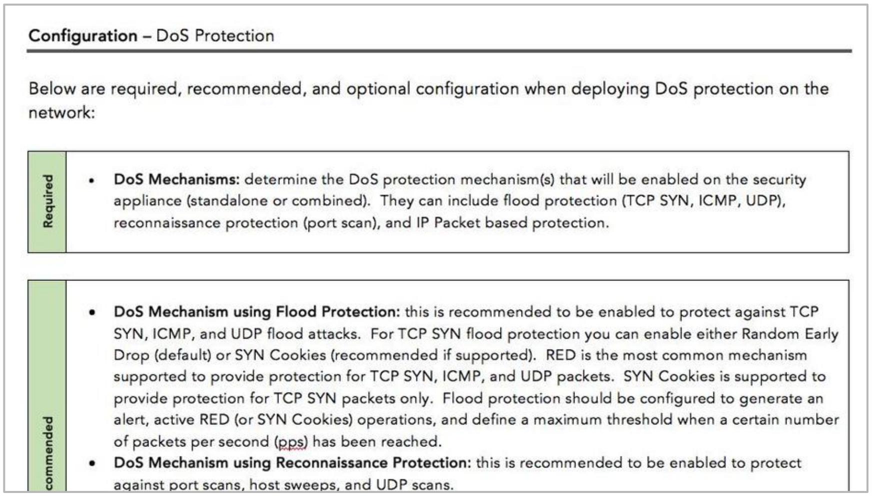
Required

- **Subscription & Licensing:** make sure to activate and license all security features that will be configured on the firewall appliance to receive the most recent attack signatures and updates.
- **Allowed / Blocked File Types:** determine what file types should be allowed (or blocked) on the firewall appliance.
- **Reputation List:** based on the vendor solution, determine how the reputation list will be obtained in which the firewall appliance will look at first before going through the configured security policies. This may be a list of IP address, domains, and/or URLs provided by the vendor (recommended) or an external list managed by a third-party source.
- **IPS Mode:** determine the IPS mode that will be used. The available options include Active (Block) and Passive (Monitor only) Modes.
- **Certificate for SSL/TLS Decryption (Deep Inspection):** user endpoints must trust the certificate generated on the firewall appliance using either group policies (GPO) and/or manually importing the certificate into the user's web browsers to avoid receiving a security warning.

- **Block security risk categories:** it's recommended to detect and block content for malicious sites, phishing, spyware, anonymizers, proxies, hacking, Spam URLs, Malware, Botnets, C2 (C&C), TOR (dark web), Bogon and any other critical/high security risk categories for all security features implemented.
- **Block inappropriate content categories:** it's recommended to block content for adult/mature websites such as pornography including violence, illegal activities, drugs, racism, hate, etc.
- **Block file sharing (and bandwidth consuming) categories:** it's recommended to block content for P2P and BitTorrent applications

This will show required, recommended, and optional configuration for the security features on the firewall appliance. For example, it is required for the firewall appliance to have the necessary license and subscriptions to use most of the security features listed in this POD. One of the recommendations include block websites/applications in high security risk categories. Or access to inappropriate content and file sharing categories among others.

There is another configuration POD that is focused on DoS Protection if that security feature will be enabled (and supported) on the firewall appliance:



Configuration – DoS Protection

Below are required, recommended, and optional configuration when deploying DoS protection on the network:

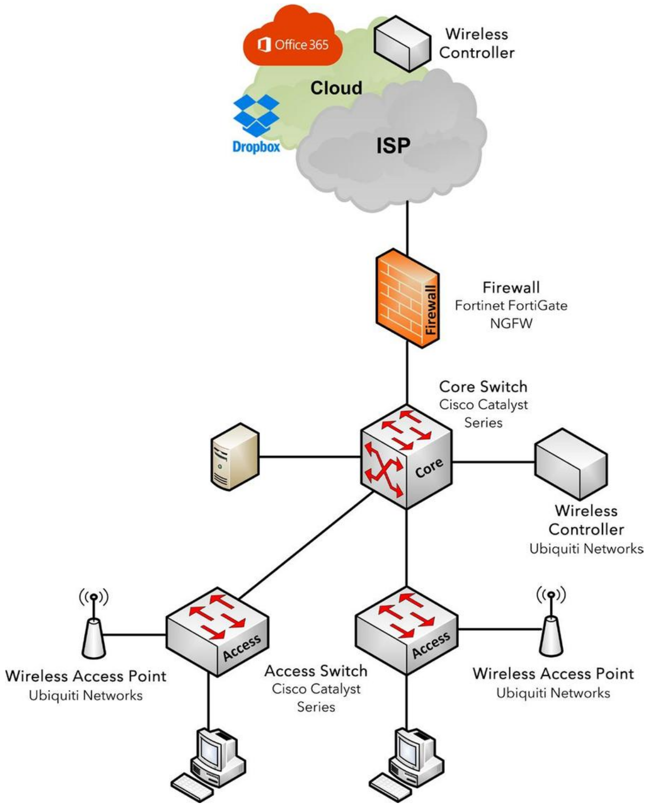
Required

- **DoS Mechanisms:** determine the DoS protection mechanism(s) that will be enabled on the security appliance (standalone or combined). They can include flood protection (TCP SYN, ICMP, UDP), reconnaissance protection (port scan), and IP Packet based protection.

commended

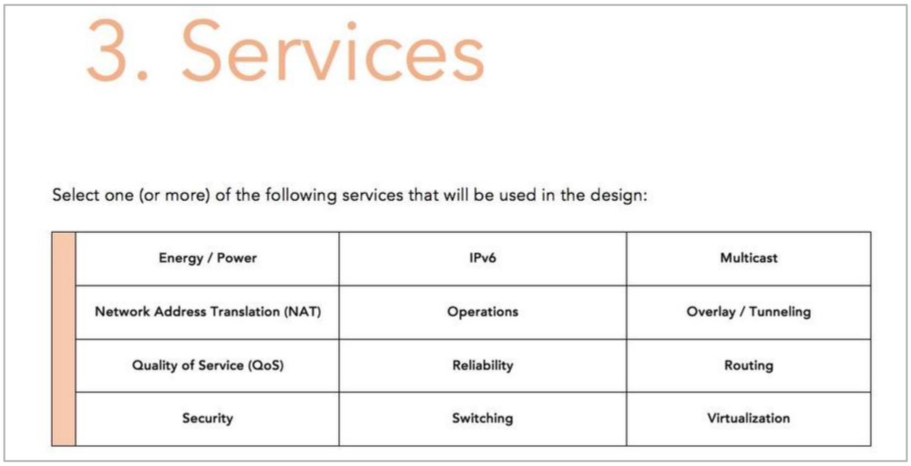
- **DoS Mechanism using Flood Protection:** this is recommended to be enabled to protect against TCP SYN, ICMP, and UDP flood attacks. For TCP SYN flood protection you can enable either Random Early Drop (default) or SYN Cookies (recommended if supported). RED is the most common mechanism supported to provide protection for TCP SYN, ICMP, and UDP packets. SYN Cookies is supported to provide protection for TCP SYN packets only. Flood protection should be configured to generate an alert, active RED (or SYN Cookies) operations, and define a maximum threshold when a certain number of packets per second (pps) has been reached.
- **DoS Mechanism using Reconnaissance Protection:** this is recommended to be enabled to protect against port scans, host sweeps, and UDP scans.

At this stage we are done with everything that is required for the Security POD. As a result here is our updated customer design:



(Step 3) Services

Once we are done with the solution design we can continue on with the service design:



3. Services

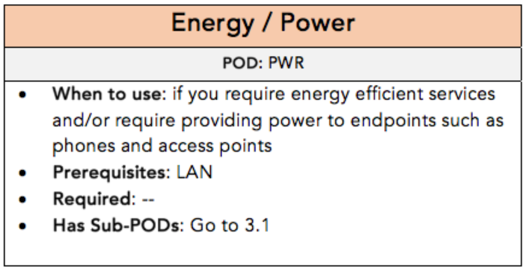
Select one (or more) of the following services that will be used in the design:

Energy / Power	IPv6	Multicast
Network Address Translation (NAT)	Operations	Overlay / Tunneling
Quality of Service (QoS)	Reliability	Routing
Security	Switching	Virtualization

Here we need to select one or more of the service PODs that are listed here. We know that from our foundation and solution design, the following services are required:

- Routing
- Switching
- POE
- DHCP
- NAT

Let's focus on those for our customer design. Among the service PODs, let's start with the "Energy / Power" POD which is where "POE" is located

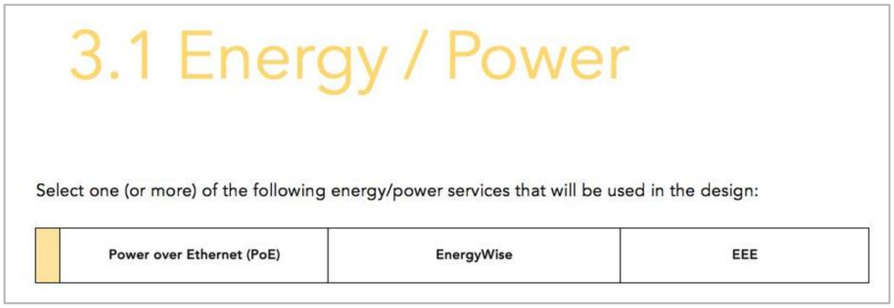


Energy / Power

POD: PWR

- **When to use**: if you require energy efficient services and/or require providing power to endpoints such as phones and access points
- **Prerequisites**: LAN
- **Required**: --
- **Has Sub-PODs**: Go to 3.1

The only prerequisite here is the LAN POD. Therefore lets go to section 3.1

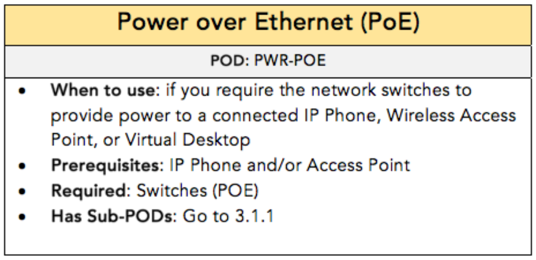


3.1 Energy / Power

Select one (or more) of the following energy/power services that will be used in the design:

🟨	Power over Ethernet (PoE)	EnergyWise	EEE

Here we need to select one or more of the following PODs. For our design, we require the POE POD which is required to work with our Wireless POD.



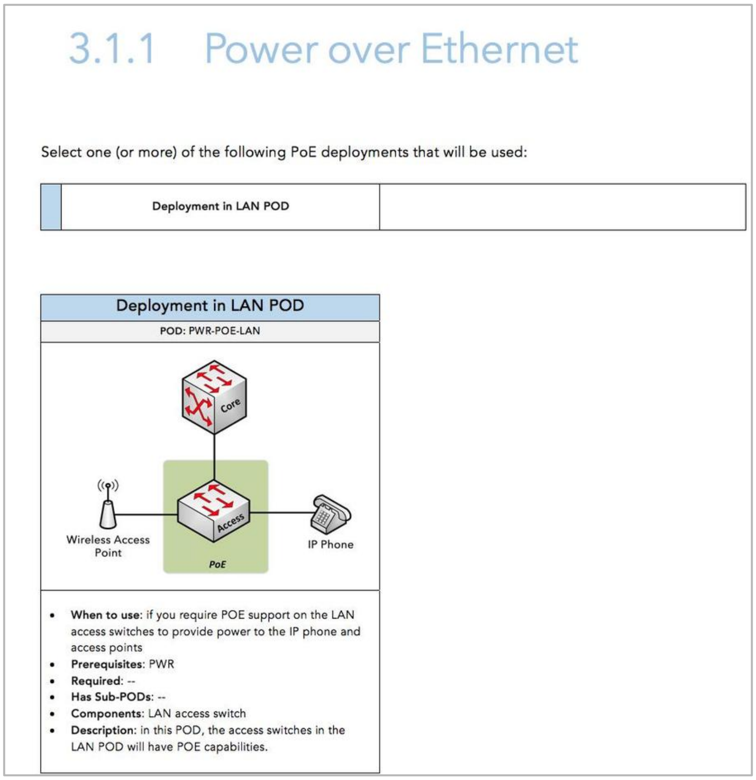
Power over Ethernet (PoE)

POD: PWR-POE

- **When to use:** if you require the network switches to provide power to a connected IP Phone, Wireless Access Point, or Virtual Desktop
- **Prerequisites:** IP Phone and/or Access Point
- **Required:** Switches (POE)
- **Has Sub-PODs:** Go to 3.1.1

This has a prerequisite for having either IP phones and/or access points. Well, we do have access point components that exist within the Wireless POD and it will require the access switches to support PoE.

Let's continue on to the sub-PODs:



3.1.1 Power over Ethernet

Select one (or more) of the following PoE deployments that will be used:

🟦	Deployment in LAN POD	

Deployment in LAN POD

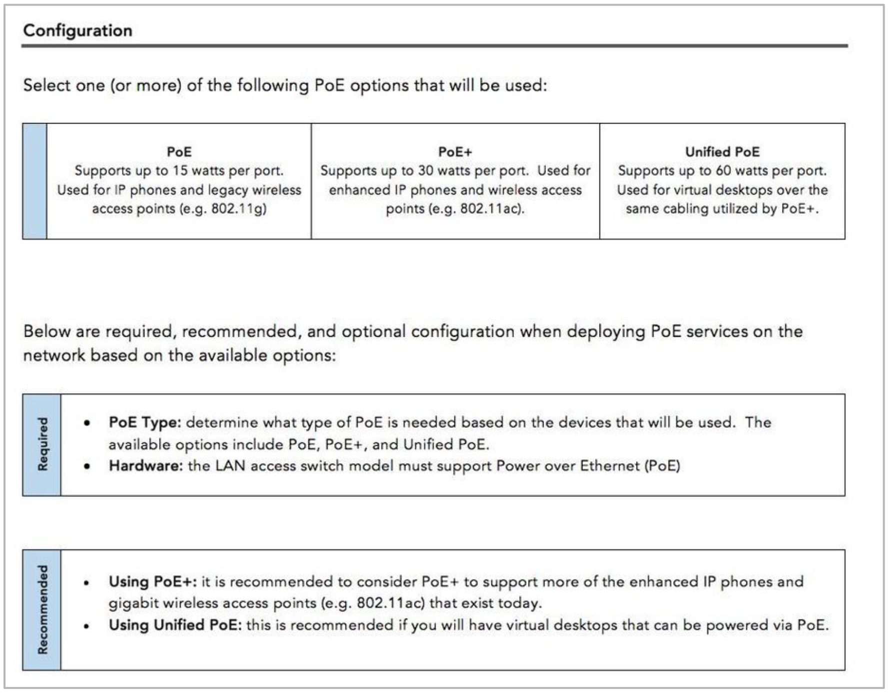
POD: PWR-POE-LAN

- **When to use**: if you require POE support on the LAN access switches to provide power to the IP phone and access points
- **Prerequisites**: PWR
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: LAN access switch
- **Description**: in this POD, the access switches in the LAN POD will have POE capabilities.

This will show how POE can be deployed on the network which is common within the LAN which is what we are using. This deployment shows that the IP phones and access points should be connected to POE enabled access switches in the LAN POD.

As we move down in this section, we reach the configuration POD section:

This will show the available POE options that are supported including how it can be configured (or used) on the LAN access switches.



Configuration

Select one (or more) of the following PoE options that will be used:

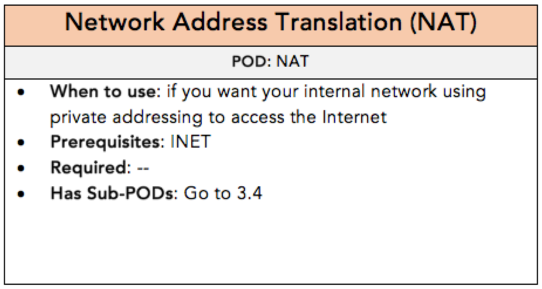
PoE	PoE+	Unified PoE
Supports up to 15 watts per port. Used for IP phones and legacy wireless access points (e.g. 802.11g)	Supports up to 30 watts per port. Used for enhanced IP phones and wireless access points (e.g. 802.11ac).	Supports up to 60 watts per port. Used for virtual desktops over the same cabling utilized by PoE+.

Below are required, recommended, and optional configuration when deploying PoE services on the network based on the available options:

Required	• **PoE Type:** determine what type of PoE is needed based on the devices that will be used. The available options include PoE, PoE+, and Unified PoE. • **Hardware:** the LAN access switch model must support Power over Ethernet (PoE)

Recommended	• **Using PoE+:** it is recommended to consider PoE+ to support more of the enhanced IP phones and gigabit wireless access points (e.g. 802.11ac) that exist today. • **Using Unified PoE:** this is recommended if you will have virtual desktops that can be powered via PoE.

The next service POD will be NAT which was determined while building the Internet and Firewall PODs:

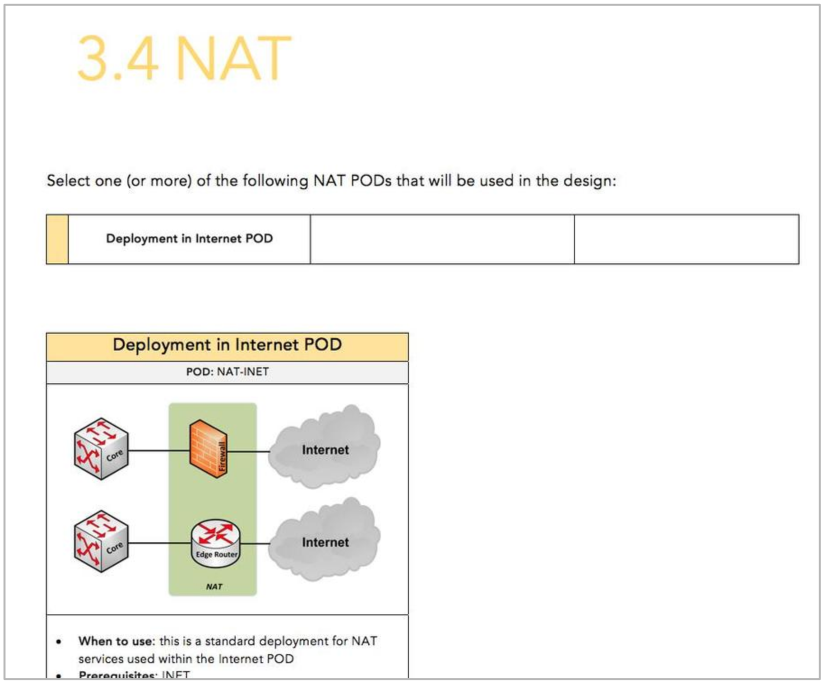


Network Address Translation (NAT)

POD: NAT

- **When to use**: if you want your internal network using private addressing to access the Internet
- **Prerequisites**: INET
- **Required**: --
- **Has Sub-PODs**: Go to 3.4

This has a prerequisite for the Internet POD and it has sub-PODs available:



3.4 NAT

Select one (or more) of the following NAT PODs that will be used in the design:

Deployment in Internet POD		

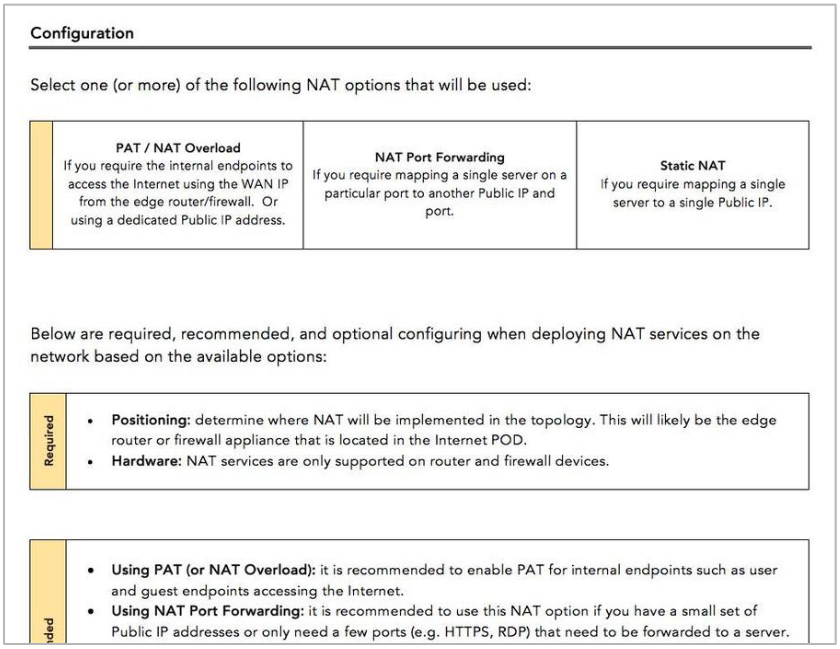
Deployment in Internet POD

POD: NAT-INET

- **When to use**: this is a standard deployment for NAT services used within the Internet POD
- **Prerequisites**: INET

This will show how NAT can be deployed on the network which is common within the Internet POD. The POD details will show how they are deployed along with other details we can reference.

There is also a configuration POD section available:



Configuration

Select one (or more) of the following NAT options that will be used:

PAT / NAT Overload If you require the internal endpoints to access the Internet using the WAN IP from the edge router/firewall. Or using a dedicated Public IP address.	**NAT Port Forwarding** If you require mapping a single server on a particular port to another Public IP and port.	**Static NAT** If you require mapping a single server to a single Public IP.

Below are required, recommended, and optional configuring when deploying NAT services on the network based on the available options:

Required

- **Positioning:** determine where NAT will be implemented in the topology. This will likely be the edge router or firewall appliance that is located in the Internet POD.
- **Hardware:** NAT services are only supported on router and firewall devices.

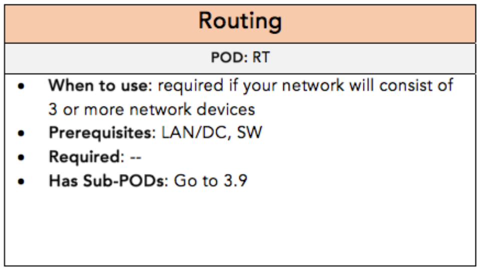
nded

- **Using PAT (or NAT Overload):** it is recommended to enable PAT for internal endpoints such as user and guest endpoints accessing the Internet.
- **Using NAT Port Forwarding:** it is recommended to use this NAT option if you have a small set of Public IP addresses or only need a few ports (e.g. HTTPS, RDP) that need to be forwarded to a server.

This will show the NAT options including the required, recommended, and optional configuration for NAT on the firewall appliance in our topology. For example, it is required for us to determine where NAT services will be configured which will likely be the edge router or firewall. And it is recommended to configure NAT port forwarding if you have a small set of Public IP addresses or only need a few ports (e.g. HTTPS, RDP) to be forwarded to a server.

At this stage, we are done with our NAT POD.

The next service POD will be the Routing POD based on our requirements.



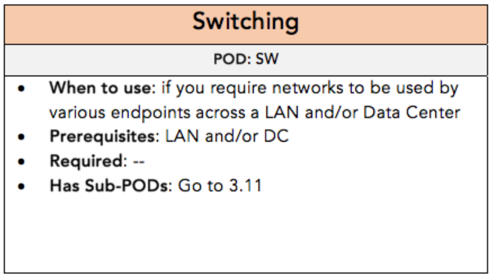
Routing

POD: RT

- **When to use**: required if your network will consist of 3 or more network devices
- **Prerequisites**: LAN/DC, SW
- **Required**: --
- **Has Sub-PODs**: Go to 3.9

This has a prerequisite for a LAN or DC POD including the Switching POD (if it is already added to our list). Therefore, we will come back to this POD once we complete our Switching POD.

Let's review the Switching POD details further:

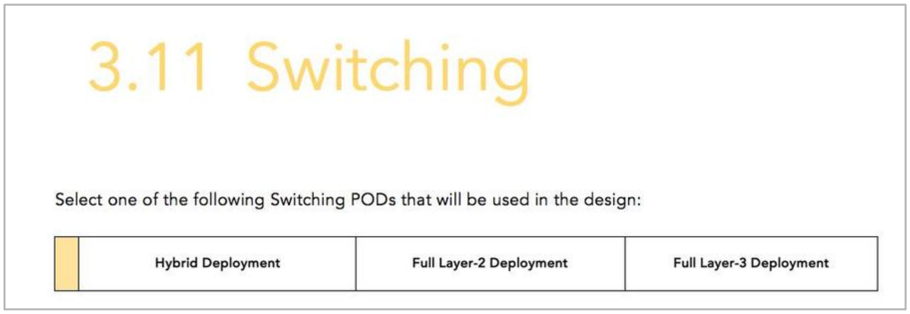


Switching

POD: SW

- **When to use**: if you require networks to be used by various endpoints across a LAN and/or Data Center
- **Prerequisites**: LAN and/or DC
- **Required**: --
- **Has Sub-PODs**: Go to 3.11

This has a prerequisite for a LAN or DC POD which we already have, so let's go to the available sub-PODs:



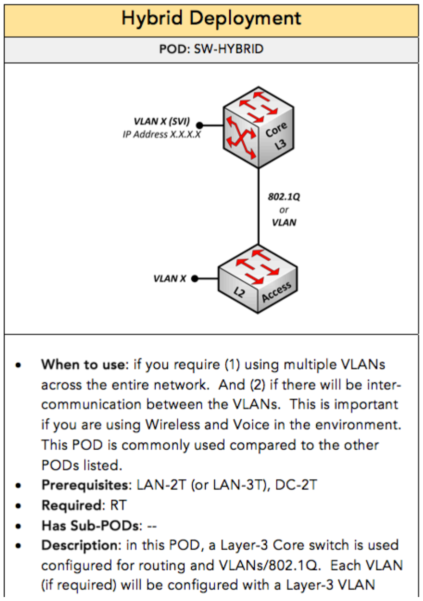
3.11 Switching

Select one of the following Switching PODs that will be used in the design:

Hybrid Deployment	Full Layer-2 Deployment	Full Layer-3 Deployment

Great, now here we need to determine which Switching deployment will be used among the LAN POD. This can be a hybrid, full Layer-2, or full Layer-3 deployment. It is important to look at each POD to determine which one will align with the business requirements and match your preference as the network architect/engineer. If you remember the example I gave in the beginning, if you want minimal layer-2 then you might choose the "Full Layer-3 Deployment" POD.

However, for our design I will choose the Hybrid Deployment which is the most common and allows us to extend the various networks (configured as VLANs) across our LAN. This means, by referencing the details in this POD, the Core switch would be a Layer-3 switch and our access switches will be Layer-2 switches.



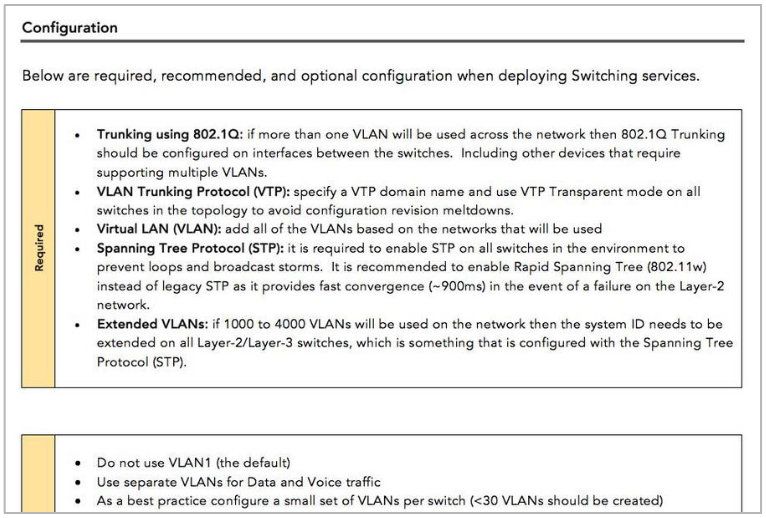
Hybrid Deployment

POD: SW-HYBRID

- **When to use**: if you require (1) using multiple VLANs across the entire network. And (2) if there will be inter-communication between the VLANs. This is important if you are using Wireless and Voice in the environment. This POD is commonly used compared to the other PODs listed.
- **Prerequisites**: LAN-2T (or LAN-3T), DC-2T
- **Required**: RT
- **Has Sub-PODs**: --
- **Description**: in this POD, a Layer-3 Core switch is used configured for routing and VLANs/802.1Q. Each VLAN (if required) will be configured with a Layer-3 VLAN

You will also see that using this POD has a prerequisite for the LAN-2T (or LAN-3T) POD. If you remember, our LAN POD is using a Traditional 2-Tier topology so we can use this switching POD for our topology. We also see that the Routing POD is required which is great because we already have this on our list.

As we moved down to the Configuration POD in this section:



Configuration

Below are required, recommended, and optional configuration when deploying Switching services.

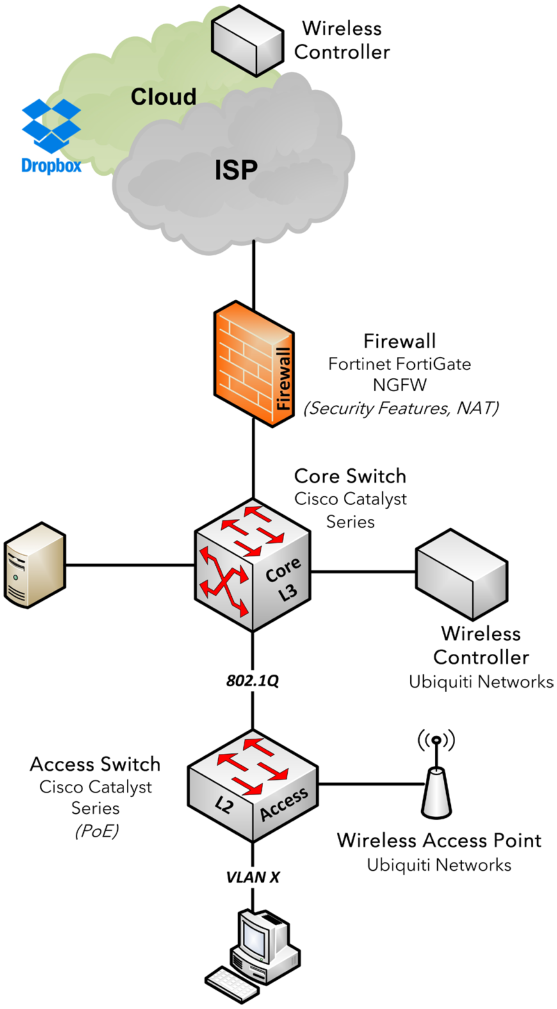
Required

- **Trunking using 802.1Q:** if more than one VLAN will be used across the network then 802.1Q Trunking should be configured on interfaces between the switches. Including other devices that require supporting multiple VLANs.
- **VLAN Trunking Protocol (VTP):** specify a VTP domain name and use VTP Transparent mode on all switches in the topology to avoid configuration revision meltdowns.
- **Virtual LAN (VLAN):** add all of the VLANs based on the networks that will be used
- **Spanning Tree Protocol (STP):** it is required to enable STP on all switches in the environment to prevent loops and broadcast storms. It is recommended to enable Rapid Spanning Tree (802.11w) instead of legacy STP as it provides fast convergence (~900ms) in the event of a failure on the Layer-2 network.
- **Extended VLANs:** if 1000 to 4000 VLANs will be used on the network then the system ID needs to be extended on all Layer-2/Layer-3 switches, which is something that is configured with the Spanning Tree Protocol (STP).

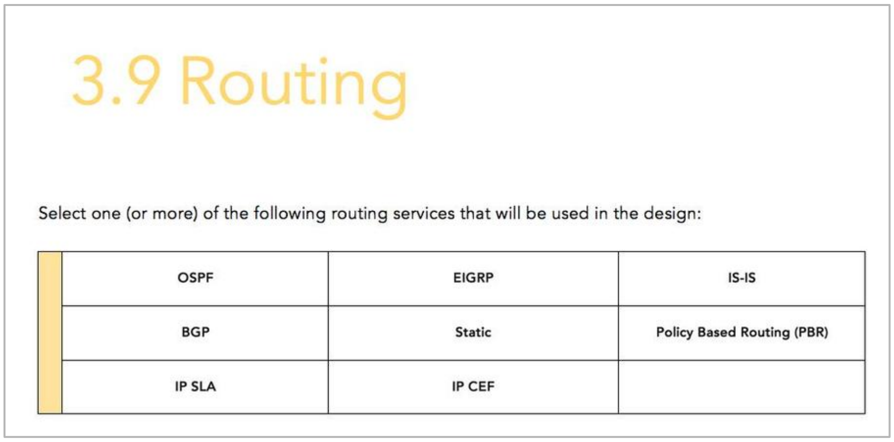
- Do not use VLAN1 (the default)
- Use separate VLANs for Data and Voice traffic
- As a best practice configure a small set of VLANs per switch (<30 VLANs should be created)

We can see what configuration is required, recommended, and optional within the Switching POD. For example, we see that it is required to enable VTP and STP on all of the LAN switches. It is recommended to not use VLAN 1 for user/server traffic. And it is recommended to use VTP transparent mode on all the switches due VTP configuration revision related issues. Again, the available configuration PODs provide a guideline for how we should configure the devices on our network.

At this stage, we are finished with the Switching POD which will give us the following network topology:



Now let's complete the Routing POD and we see it has sub-PODs available. Therefore, let's go to section 3.9



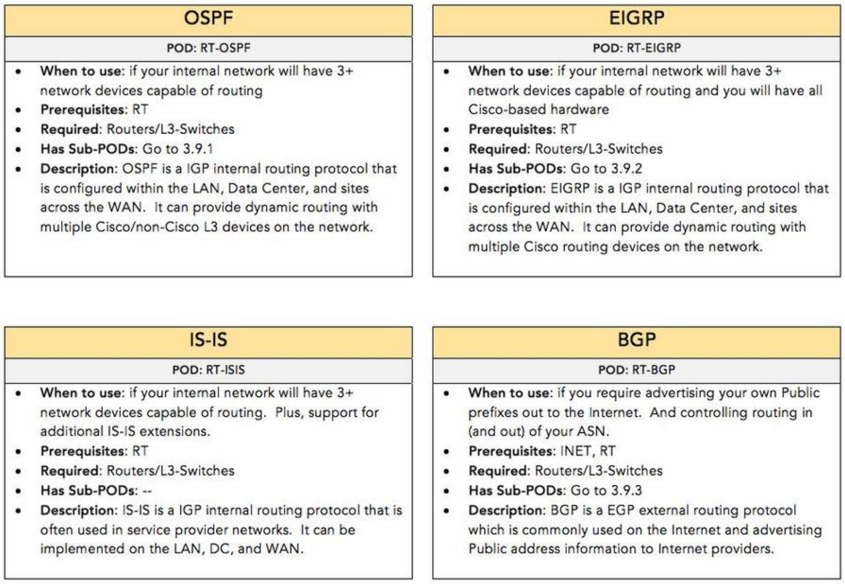
3.9 Routing

Select one (or more) of the following routing services that will be used in the design:

OSPF	EIGRP	IS-IS
BGP	Static	Policy Based Routing (PBR)
IP SLA	IP CEF	

Here we need to select one (or more) of the following routing services that will be used in the design. We need to look at each POD to determine which ones would apply for our customer design. Most of the PODs "When to use" states if we have 3 or more Layer-3 network devices (e.g. L3-Switch, Router, Firewall).

For our customer design, we only have two Layer-3 devices. This means we can omit the OSPF, EIGRP, and IS-IS routing PODs. We also don't require the BGP POD since we are not advertising any subnets that we own.



OSPF

POD: RT-OSPF

- **When to use**: if your internal network will have 3+ network devices capable of routing
- **Prerequisites**: RT
- **Required**: Routers/L3-Switches
- **Has Sub-PODs**: Go to 3.9.1
- **Description**: OSPF is a IGP internal routing protocol that is configured within the LAN, Data Center, and sites across the WAN. It can provide dynamic routing with multiple Cisco/non-Cisco L3 devices on the network.

EIGRP

POD: RT-EIGRP

- **When to use**: if your internal network will have 3+ network devices capable of routing and you will have all Cisco-based hardware
- **Prerequisites**: RT
- **Required**: Routers/L3-Switches
- **Has Sub-PODs**: Go to 3.9.2
- **Description**: EIGRP is a IGP internal routing protocol that is configured within the LAN, Data Center, and sites across the WAN. It can provide dynamic routing with multiple Cisco routing devices on the network.

IS-IS

POD: RT-ISIS

- **When to use**: if your internal network will have 3+ network devices capable of routing. Plus, support for additional IS-IS extensions.
- **Prerequisites**: RT
- **Required**: Routers/L3-Switches
- **Has Sub-PODs**: --
- **Description**: IS-IS is a IGP internal routing protocol that is often used in service provider networks. It can be implemented on the LAN, DC, and WAN.

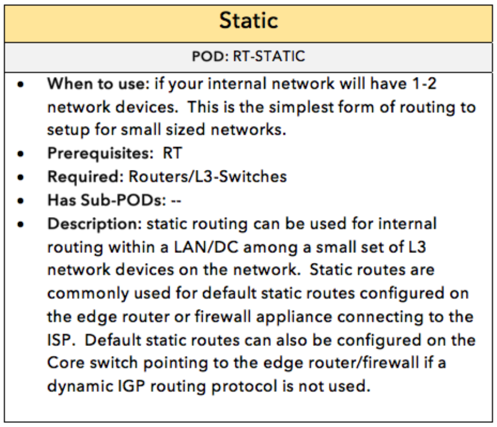
BGP

POD: RT-BGP

- **When to use**: if you require advertising your own Public prefixes out to the Internet. And controlling routing in (and out) of your ASN.
- **Prerequisites**: INET, RT
- **Required**: Routers/L3-Switches
- **Has Sub-PODs**: Go to 3.9.3
- **Description**: BGP is a EGP external routing protocol which is commonly used on the Internet and advertising Public address information to Internet providers.

Furthermore, we do not have a direct requirement or need to use PBR, IP SLA, or IP CEF so those PODs will also be omitted.

We will select the "Static" POD because our topology does have 1-2 network devices. This means that static routing must be configured between the L3-Core switch and the firewall in which is mentioned in the description.

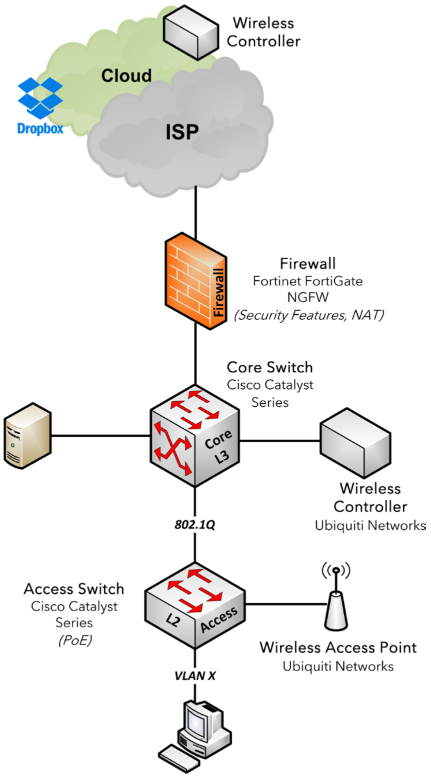


Static

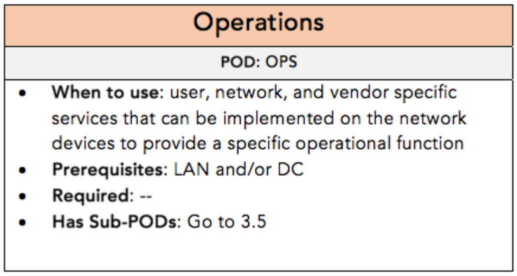
POD: RT-STATIC

- **When to use:** if your internal network will have 1-2 network devices. This is the simplest form of routing to setup for small sized networks.
- **Prerequisites:** RT
- **Required:** Routers/L3-Switches
- **Has Sub-PODs:** --
- **Description:** static routing can be used for internal routing within a LAN/DC among a small set of L3 network devices on the network. Static routes are commonly used for default static routes configured on the edge router or firewall appliance connecting to the ISP. Default static routes can also be configured on the Core switch pointing to the edge router/firewall if a dynamic IGP routing protocol is not used.

Since there are no sub-PODs for static routing, we are finished with the Routing POD giving us the same network topology.



We still have one more service POD to complete and that is the DHCP POD. So let's go back to the main service page:



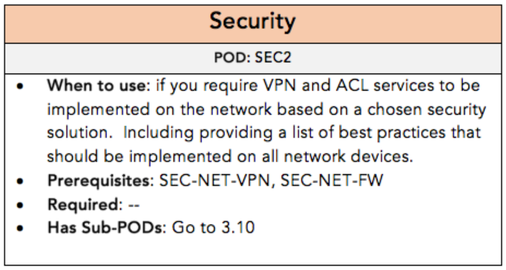
Operations

POD: OPS

- **When to use**: user, network, and vendor specific services that can be implemented on the network devices to provide a specific operational function
- **Prerequisites**: LAN and/or DC
- **Required**: --
- **Has Sub-PODs**: Go to 3.5

The DHCP POD is located under "Operations" which has a lot of other services we can consider.

Just like what we did for the solution design, we can include additional services based on our recommendations and preferences as a the network architect/engineer. One of these services that we will include is the security services:

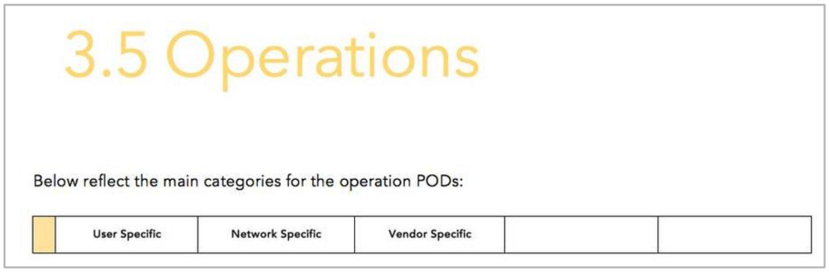


Security

POD: SEC2

- **When to use**: if you require VPN and ACL services to be implemented on the network based on a chosen security solution. Including providing a list of best practices that should be implemented on all network devices.
- **Prerequisites**: SEC-NET-VPN, SEC-NET-FW
- **Required**: --
- **Has Sub-PODs**: Go to 3.10

We will also explore the services under the Operations category to see what else can be included:



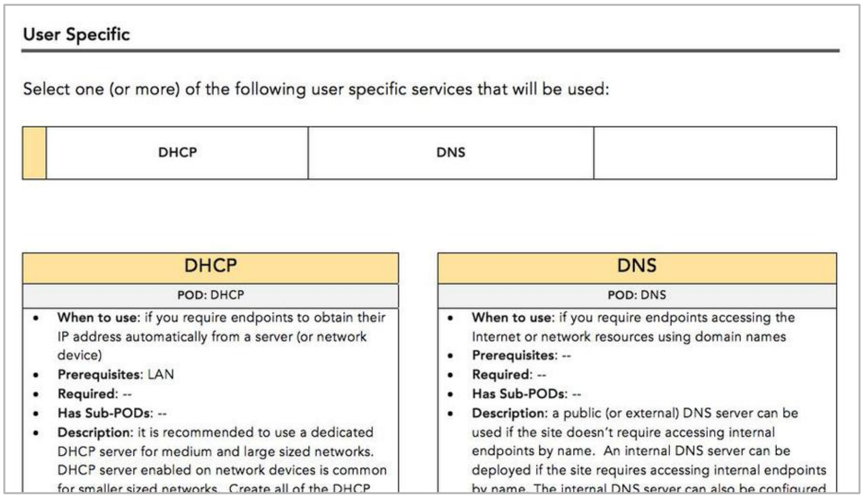
3.5 Operations

Below reflect the main categories for the operation PODs:

🟨	User Specific	Network Specific	Vendor Specific		

This will start off listing the major category sections from User, network, to vendor specific operational services.

First off, under User Specific services, we see DHCP listed so let's select that POD



User Specific

Select one (or more) of the following user specific services that will be used:

DHCP	DNS	

DHCP

POD: DHCP

- **When to use:** if you require endpoints to obtain their IP address automatically from a server (or network device)
- **Prerequisites:** LAN
- **Required:** --
- **Has Sub-PODs:** --
- **Description:** it is recommended to use a dedicated DHCP server for medium and large sized networks. DHCP server enabled on network devices is common for smaller sized networks. Create all of the DHCP

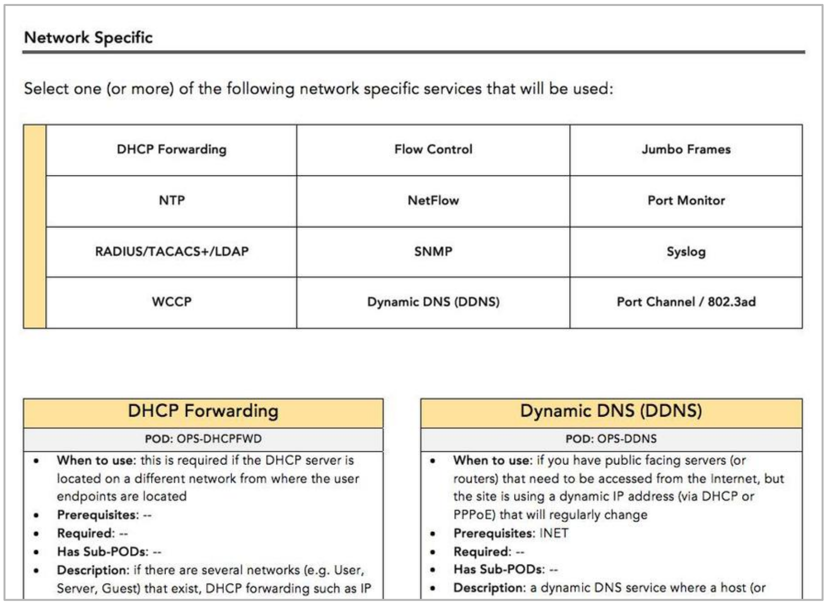
DNS

POD: DNS

- **When to use:** if you require endpoints accessing the Internet or network resources using domain names
- **Prerequisites:** --
- **Required:** --
- **Has Sub-PODs:** --
- **Description:** a public (or external) DNS server can be used if the site doesn't require accessing internal endpoints by name. An internal DNS server can be deployed if the site requires accessing internal endpoints by name. The internal DNS server can also be configured

There are no additional sub-PODs, but the description provides information and best practices in regards to DHCP deployment in general.

Back on the Services - Operations page. Let's look under the Network specific services:



Network Specific

Select one (or more) of the following network specific services that will be used:

DHCP Forwarding	Flow Control	Jumbo Frames
NTP	NetFlow	Port Monitor
RADIUS/TACACS+/LDAP	SNMP	Syslog
WCCP	Dynamic DNS (DDNS)	Port Channel / 802.3ad

DHCP Forwarding

POD: OPS-DHCPFWD

- **When to use:** this is required if the DHCP server is located on a different network from where the user endpoints are located
- **Prerequisites:** --
- **Required:** --
- **Has Sub-PODs:** --
- **Description:** if there are several networks (e.g. User, Server, Guest) that exist, DHCP forwarding such as IP

Dynamic DNS (DDNS)

POD: OPS-DDNS

- **When to use:** if you have public facing servers (or routers) that need to be accessed from the Internet, but the site is using a dynamic IP address (via DHCP or PPPoE) that will regularly change
- **Prerequisites:** INET
- **Required:** --
- **Has Sub-PODs:** --
- **Description:** a dynamic DNS service where a host (or

These reflect services that are primarily used by the network devices themselves. Here we would need to look at each POD to determine if that service POD should be used. Most will not point to any additional sub-PODs like DHCP. But they will still provide details for when that service should be configured along with any other best practices.

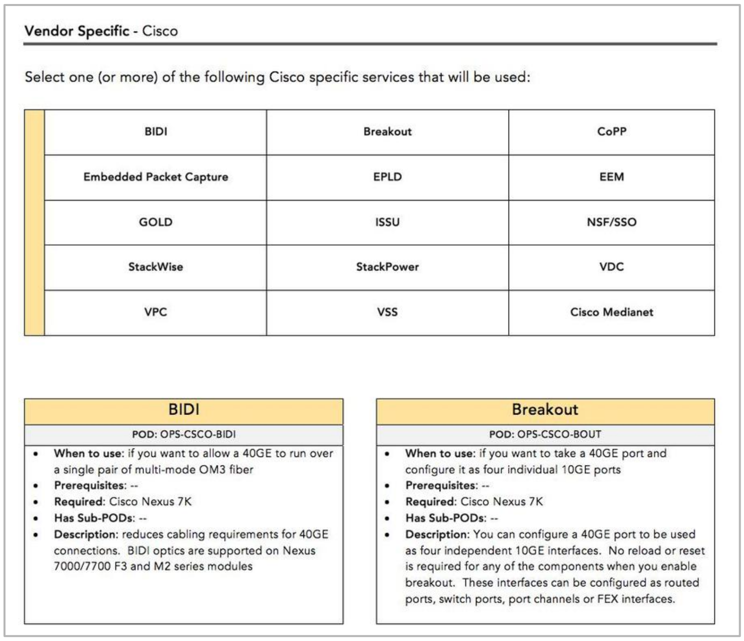
For our customer design, we will select the following PODs:

- SNMP
- Syslog
- NTP

We included the SNMP and Syslog PODs because we already included the Network Management solution. And if we select the NMS POD that will require SNMP and Syslog. Therefore, we know that we need to configure SNMP and Syslog services on all of our network devices in the topology.

NTP was added as a best practice to provide accurate timestamps among the network devices and any logs that are generated.

The other service PODs are not needed nor required for our customer design. Let's review the Vendor Specific services listed in this design cookbook:



Vendor Specific - Cisco

Select one (or more) of the following Cisco specific services that will be used:

BIDI	Breakout	CoPP
Embedded Packet Capture	EPLD	EEM
GOLD	ISSU	NSF/SSO
StackWise	StackPower	VDC
VPC	VSS	Cisco Medianet

BIDI

POD: OPS-CSCO-BIDI

- **When to use**: if you want to allow a 40GE to run over a single pair of multi-mode OM3 fiber
- **Prerequisites**: --
- **Required**: Cisco Nexus 7K
- **Has Sub-PODs**: --
- **Description**: reduces cabling requirements for 40GE connections. BIDI optics are supported on Nexus 7000/7700 F3 and M2 series modules

Breakout

POD: OPS-CSCO-BOUT

- **When to use**: if you want to take a 40GE port and configure it as four individual 10GE ports
- **Prerequisites**: --
- **Required**: Cisco Nexus 7K
- **Has Sub-PODs**: --
- **Description**: You can configure a 40GE port to be used as four independent 10GE interfaces. No reload or reset is required for any of the components when you enable breakout. These interfaces can be configured as routed ports, switch ports, port channels or FEX interfaces.

This will show a long list of services that are specifically configured on Cisco products. This means other vendor specific sections can easily be added here listing services only supported on their specific products. Among the list of Cisco vendor specific services none of these are required nor needed in our environment. Besides if there is a Cisco service that is required they will likely be listed as a requirement for that POD such as VSS and VPC.

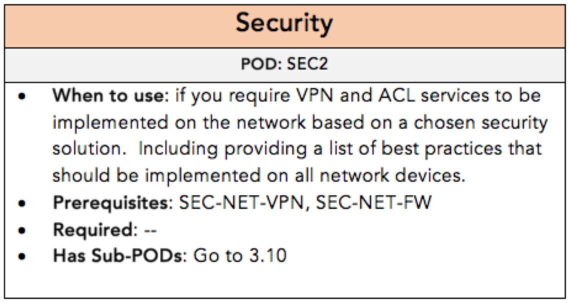
Furthermore, most of these services are only supported on certain Cisco hardware devices such as the Cisco Nexus series. This will include services such as BIDI, Breakout, VPC, and VDC. We know that we are not using Cisco Nexus hardware because that is typically used for Data Center frameworks not LANs.

Lastly, just because we don't add any of these services initially to our design, doesn't mean we can't go back to the list of operation services to determine what services we could use. For example, let’s say we are using a Chassis-based or Stack-based switch for the hardware in the LAN. Well, we could go back to the services page and determine what additional services we could implement along with any best practices that are provided.

If we are using a Cisco Stack-based switch, we will learn that our hardware can support StackWise and potentially StackPower.

Services are more flexible compared to solutions and especially frameworks. Using our house example again, it’s easy to move furniture around in the house. However, it is harder if you want the kitchen to be located in a different part of the house. And it is even more difficult if you want the house to have an extra room or level. They are not impossible, but it will be very expensive and will require a lot of time to complete. The same goes for deploying networks.

Before we conclude the services POD, we also added the security service PODs:

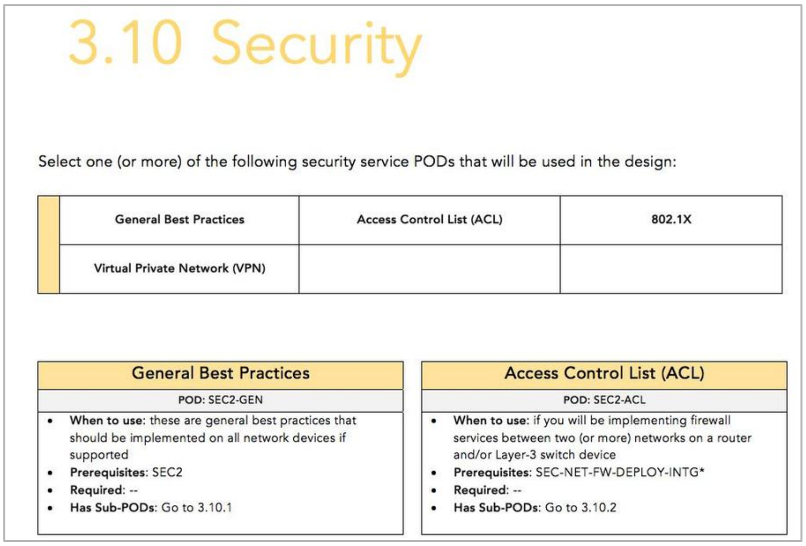


Security

POD: SEC2

- **When to use**: if you require VPN and ACL services to be implemented on the network based on a chosen security solution. Including providing a list of best practices that should be implemented on all network devices.
- **Prerequisites**: SEC-NET-VPN, SEC-NET-FW
- **Required**: --
- **Has Sub-PODs**: Go to 3.10

This doesn't have any prerequisites, so let’s go to the sub-PODs in section 3.10



3.10 Security

Select one (or more) of the following security service PODs that will be used in the design:

General Best Practices	Access Control List (ACL)	802.1X
Virtual Private Network (VPN)		

General Best Practices

POD: SEC2-GEN

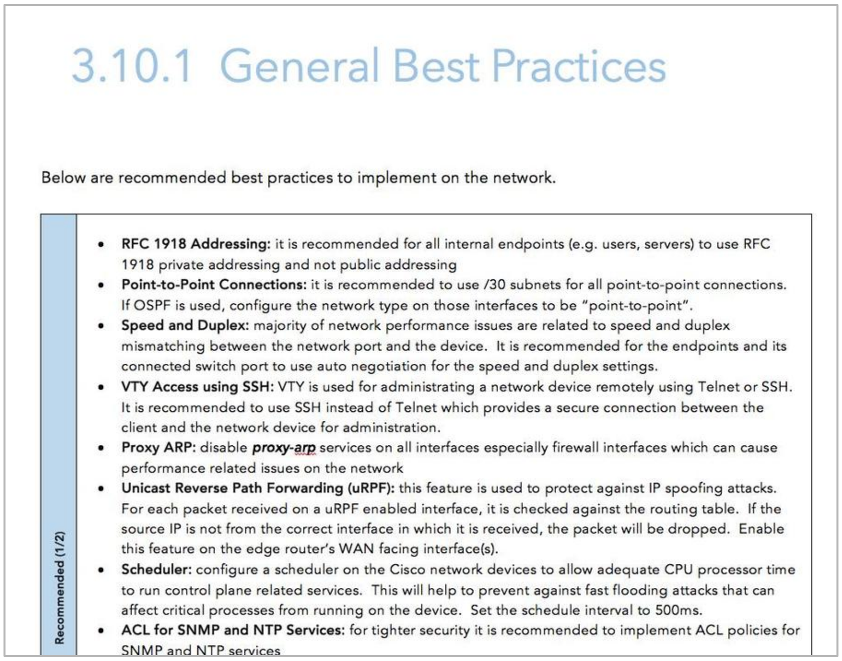
- **When to use**: these are general best practices that should be implemented on all network devices if supported
- **Prerequisites**: SEC2
- **Required**: --
- **Has Sub-PODs**: Go to 3.10.1

Access Control List (ACL)

POD: SEC2-ACL

- **When to use**: if you will be implementing firewall services between two (or more) networks on a router and/or Layer-3 switch device
- **Prerequisites**: SEC-NET-FW-DEPLOY-INTG*
- **Required**: --
- **Has Sub-PODs**: Go to 3.10.2

This will show the list of security related services we can consider. Let’s select the "General Best Practices" POD and go to its sub-PODs:



3.10.1 General Best Practices

Below are recommended best practices to implement on the network.

Recommended (1/2)

- **RFC 1918 Addressing:** it is recommended for all internal endpoints (e.g. users, servers) to use RFC 1918 private addressing and not public addressing
- **Point-to-Point Connections:** it is recommended to use /30 subnets for all point-to-point connections. If OSPF is used, configure the network type on those interfaces to be “point-to-point”.
- **Speed and Duplex:** majority of network performance issues are related to speed and duplex mismatching between the network port and the device. It is recommended for the endpoints and its connected switch port to use auto negotiation for the speed and duplex settings.
- **VTY Access using SSH:** VTY is used for administrating a network device remotely using Telnet or SSH. It is recommended to use SSH instead of Telnet which provides a secure connection between the client and the network device for administration.
- **Proxy ARP:** disable ***proxy-arp*** services on all interfaces especially firewall interfaces which can cause performance related issues on the network
- **Unicast Reverse Path Forwarding (uRPF):** this feature is used to protect against IP spoofing attacks. For each packet received on a uRPF enabled interface, it is checked against the routing table. If the source IP is not from the correct interface in which it is received, the packet will be dropped. Enable this feature on the edge router’s WAN facing interface(s).
- **Scheduler:** configure a scheduler on the Cisco network devices to allow adequate CPU processor time to run control plane related services. This will help to prevent against fast flooding attacks that can affect critical processes from running on the device. Set the schedule interval to 500ms.
- **ACL for SNMP and NTP Services:** for tighter security it is recommended to implement ACL policies for SNMP and NTP services

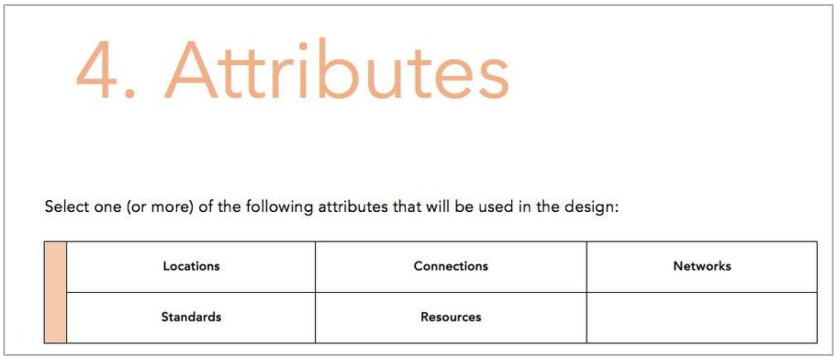
This is a simple page showing a list of recommended configuration we should implement on the network devices in the topology. These are services that the business will not think about and why they hired a network architect/engineer to provide the best possible design based on their experience. As the network architect we must consider not only the business requirements but also the technical objectives which includes:

- Performance
- Scalability
- Security
- Reliability
- Flexibility
- Network Management

If those requirements and objectives are addressed then we can include our own professional preferences to the design.

(Step 4) Attributes

At this point our design is completed, but let’s run through the design attributes to complete the finishing touches:

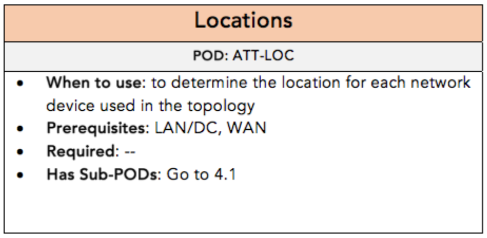


4. Attributes

Select one (or more) of the following attributes that will be used in the design:

Locations	Connections	Networks
Standards	Resources	

Here we can determine the physical location of the network devices and define the various standards that will be used. Therefore, among these attributes PODs we will select all of the listed PODs. We will first complete the location POD to determine the location for each network device in the topology design.

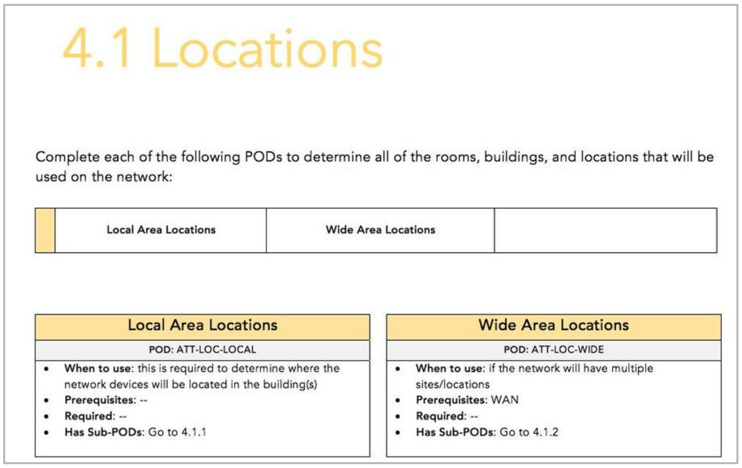


Locations

POD: ATT-LOC

- **When to use**: to determine the location for each network device used in the topology
- **Prerequisites**: LAN/DC, WAN
- **Required**: --
- **Has Sub-PODs**: Go to 4.1

This has a prerequisite for the LAN, DC, and/or WAN POD. We will go to section 4.1:



4.1 Locations

Complete each of the following PODs to determine all of the rooms, buildings, and locations that will be used on the network:

Local Area Locations	Wide Area Locations	

Local Area Locations

POD: ATT-LOC-LOCAL

- **When to use**: this is required to determine where the network devices will be located in the building(s)
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 4.1.1

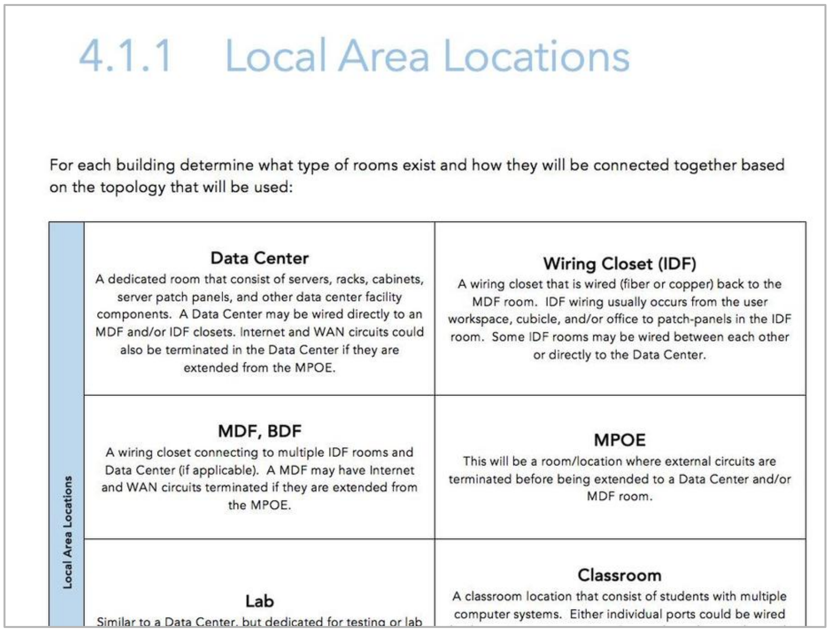
Wide Area Locations

POD: ATT-LOC-WIDE

- **When to use**: if the network will have multiple sites/locations
- **Prerequisites**: WAN
- **Required**: --
- **Has Sub-PODs**: Go to 4.1.2

Here we need to determine all of the rooms, buildings, and locations will be connected together on the network. This will be broken up as either a local location or a wide location.

We don't require the wide location POD because we do not have multiple sites. Therefore, we will select the local location POD and go to section 4.1.1



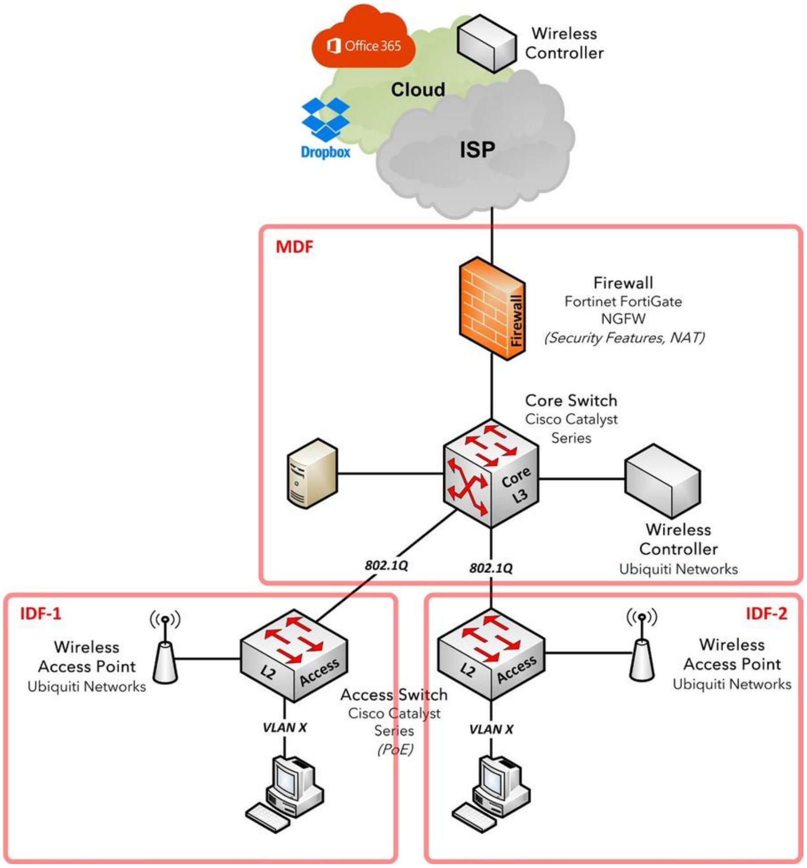
4.1.1 Local Area Locations

For each building determine what type of rooms exist and how they will be connected together based on the topology that will be used:

Local Area Locations	**Data Center** A dedicated room that consist of servers, racks, cabinets, server patch panels, and other data center facility components. A Data Center may be wired directly to an MDF and/or IDF closets. Internet and WAN circuits could also be terminated in the Data Center if they are extended from the MPOE.	**Wiring Closet (IDF)** A wiring closet that is wired (fiber or copper) back to the MDF room. IDF wiring usually occurs from the user workspace, cubicle, and/or office to patch-panels in the IDF room. Some IDF rooms may be wired between each other or directly to the Data Center.
	MDF, BDF A wiring closet connecting to multiple IDF rooms and Data Center (if applicable). A MDF may have Internet and WAN circuits terminated if they are extended from the MPOE.	**MPOE** This will be a room/location where external circuits are terminated before being extended to a Data Center and/or MDF room.
	Lab Similar to a Data Center, but dedicated for testing or lab	**Classroom** A classroom location that consist of students with multiple computer systems. Either individual ports could be wired

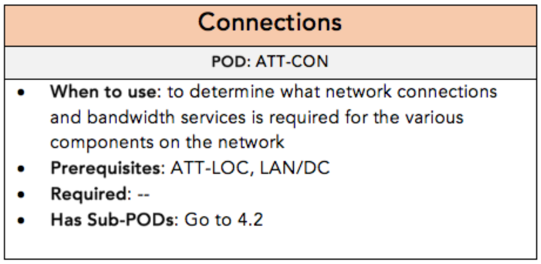
This will show a list of Grid PODs with possible room locations that our customer may have. We need to determine what type of rooms will exist and how they will be connected together based on the topology that will be used.

For our customer design, there will be single building with a MDF and two IDF rooms. The MDF room will consist of the Core switch, Firewall appliance, servers, and the Internet connection itself. Each IDF room will have a POE enabled access switch with access points and user endpoints connected.



Ethernet wiring would be connected between each IDF back to the MDF room.

Another attribute is the connection POD which is required for each network device in the topology. We need to determine the bandwidth services that will exist on that device

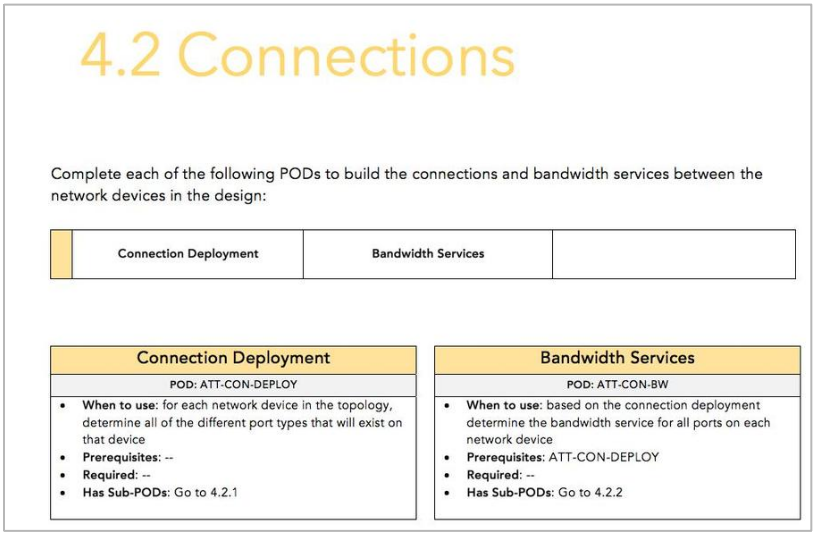


Connections

POD: ATT-CON

- **When to use**: to determine what network connections and bandwidth services is required for the various components on the network
- **Prerequisites**: ATT-LOC, LAN/DC
- **Required**: --
- **Has Sub-PODs**: Go to 4.2

This section provides a full in-depth process (plus examples) to determine the type of ports, bandwidth services, and how the network devices will be connected together.



4.2 Connections

Complete each of the following PODs to build the connections and bandwidth services between the network devices in the design:

	Connection Deployment	Bandwidth Services	

Connection Deployment

POD: ATT-CON-DEPLOY

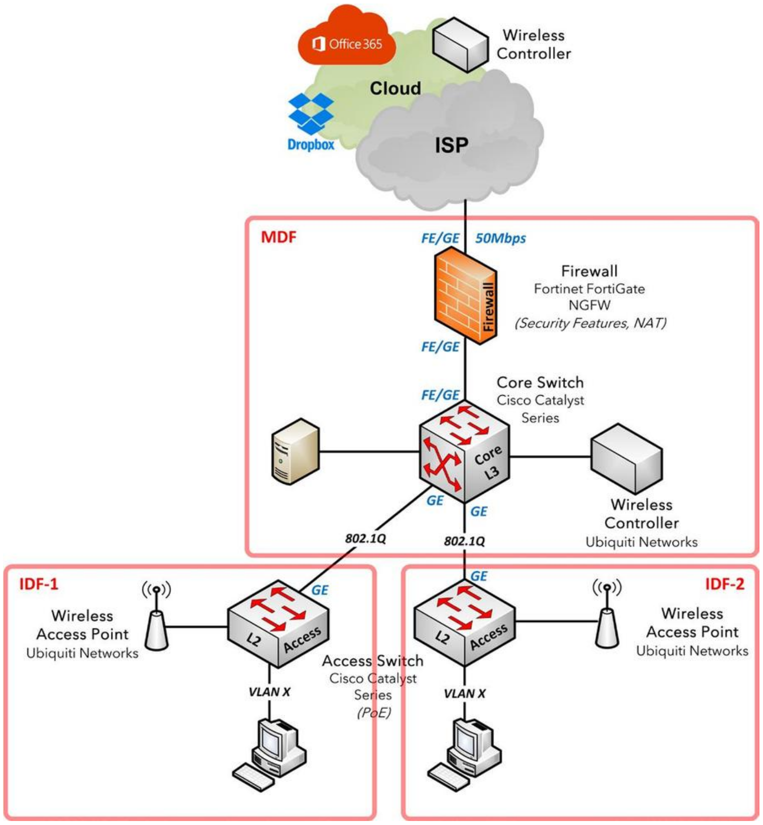
- **When to use**: for each network device in the topology, determine all of the different port types that will exist on that device
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 4.2.1

Bandwidth Services

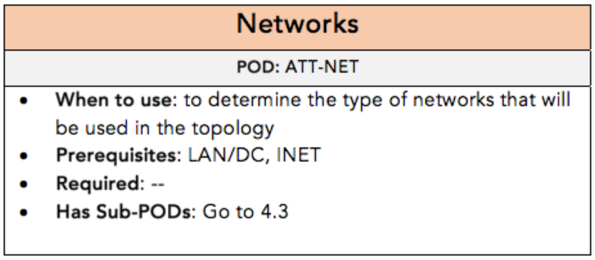
POD: ATT-CON-BW

- **When to use**: based on the connection deployment determine the bandwidth service for all ports on each network device
- **Prerequisites**: ATT-CON-DEPLOY
- **Required**: --
- **Has Sub-PODs**: Go to 4.2.2

We won't go into that here in this example, but going through that section will give us something like the following for our topology:



The next attribute involve the network POD which is used to determine the type of networks the topology will have.

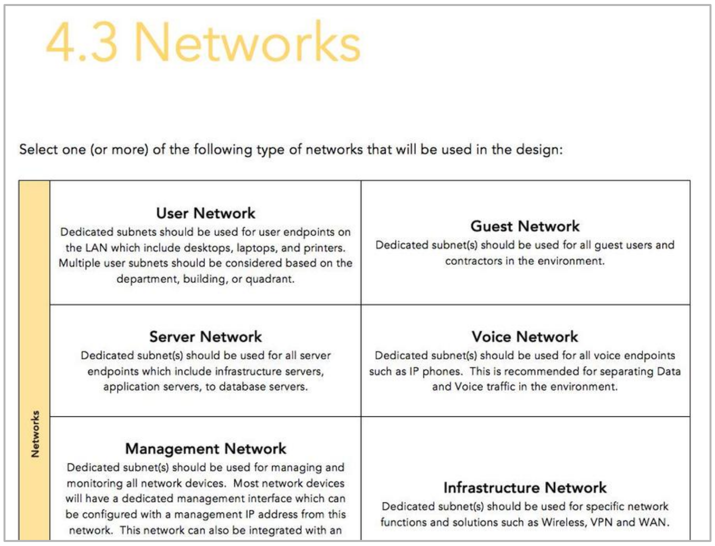


Networks

POD: ATT-NET

- **When to use:** to determine the type of networks that will be used in the topology
- **Prerequisites:** LAN/DC, INET
- **Required:** --
- **Has Sub-PODs:** Go to 4.3

When we go to section 4.3, that will show a list of possible networks that we could use and associate as a VLAN within our LAN POD.



4.3 Networks

Select one (or more) of the following type of networks that will be used in the design:

Networks	**User Network** Dedicated subnets should be used for user endpoints on the LAN which include desktops, laptops, and printers. Multiple user subnets should be considered based on the department, building, or quadrant.	**Guest Network** Dedicated subnet(s) should be used for all guest users and contractors in the environment.
	Server Network Dedicated subnet(s) should be used for all server endpoints which include infrastructure servers, application servers, to database servers.	**Voice Network** Dedicated subnet(s) should be used for all voice endpoints such as IP phones. This is recommended for separating Data and Voice traffic in the environment.
	Management Network Dedicated subnet(s) should be used for managing and monitoring all network devices. Most network devices will have a dedicated management interface which can be configured with a management IP address from this network. This network can also be integrated with an	**Infrastructure Network** Dedicated subnet(s) should be used for specific network functions and solutions such as Wireless, VPN and WAN.

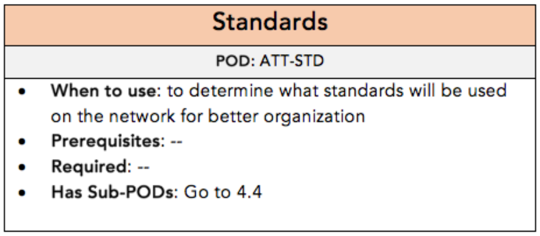
For our customer design, based on the business requirements, we will use the following networks:

- User
- Guest
- Server

As the network architect/engineer we will also include the following network(s) as a best practice:

- Management
- Transit

For the next attribute, we can determine the type of standards that will be used.



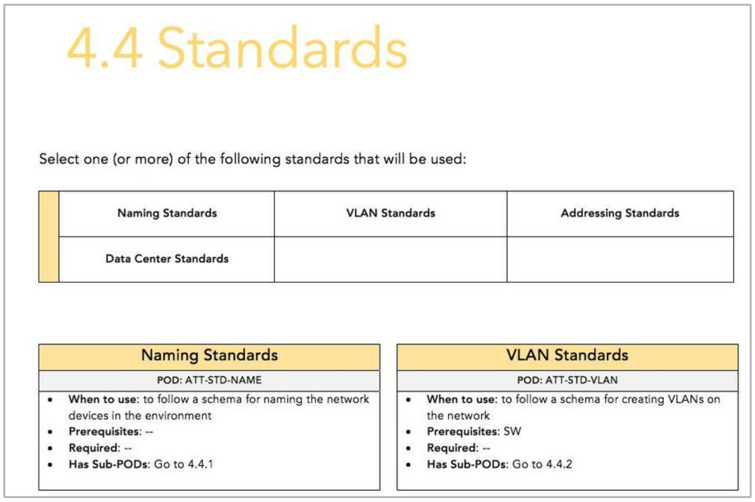
Standards

POD: ATT-STD

- **When to use**: to determine what standards will be used on the network for better organization
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 4.4

There are different standards listed in the design cookbook ranging from a naming standard, addressing standard, to even a VLAN standard.

We will skip the Data Center Standard since we only have a MDF room in the customer design. But let's cover the other standard PODs that are listed here:



4.4 Standards

Select one (or more) of the following standards that will be used:

Naming Standards	VLAN Standards	Addressing Standards
Data Center Standards		

Naming Standards

POD: ATT-STD-NAME

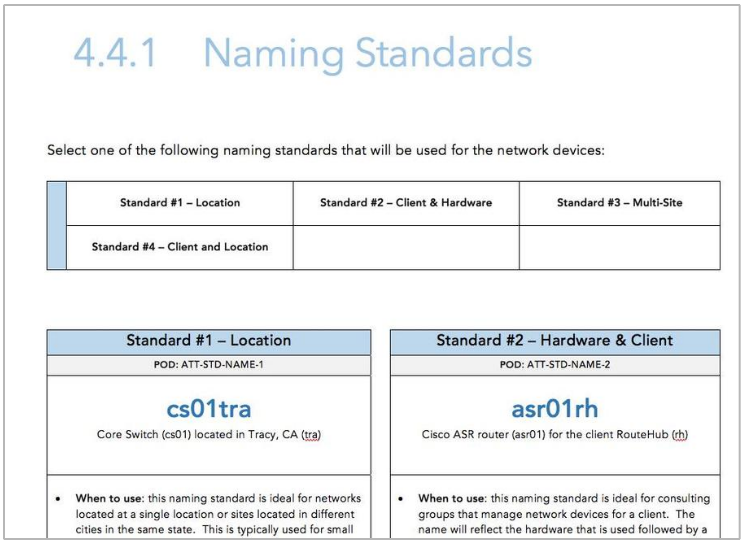
- **When to use**: to follow a schema for naming the network devices in the environment
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 4.4.1

VLAN Standards

POD: ATT-STD-VLAN

- **When to use**: to follow a schema for creating VLANs on the network
- **Prerequisites**: SW
- **Required**: --
- **Has Sub-PODs**: Go to 4.4.2

Starting with the Naming standard, we can follow a schema for naming devices on the network. There are many different schemas we could use based on the available PODs shown:



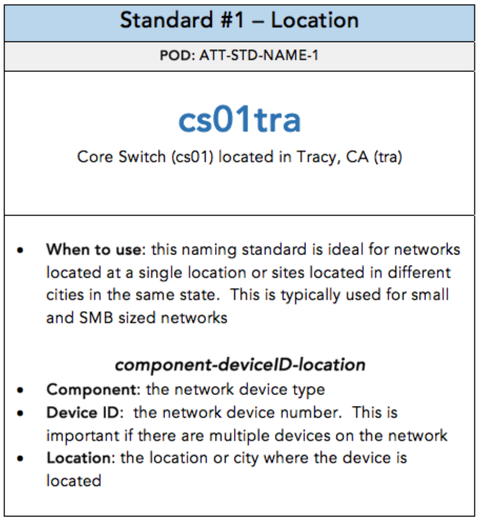
4.4.1 Naming Standards

Select one of the following naming standards that will be used for the network devices:

	Standard #1 – Location	Standard #2 – Client & Hardware	Standard #3 – Multi-Site
	Standard #4 – Client and Location		

Standard #1 – Location	Standard #2 – Hardware & Client
POD: ATT-STD-NAME-1	POD: ATT-STD-NAME-2
cs01tra Core Switch (cs01) located in Tracy, CA (tra)	**asr01rh** Cisco ASR router (asr01) for the client RouteHub (rh)
• **When to use**: this naming standard is ideal for networks located at a single location or sites located in different cities in the same state. This is typically used for small	• **When to use**: this naming standard is ideal for consulting groups that manage network devices for a client. The name will reflect the hardware that is used followed by a

For our customer design, we will keep things simple and use the "Standard #1" POD.



Standard #1 – Location

POD: ATT-STD-NAME-1

cs01tra

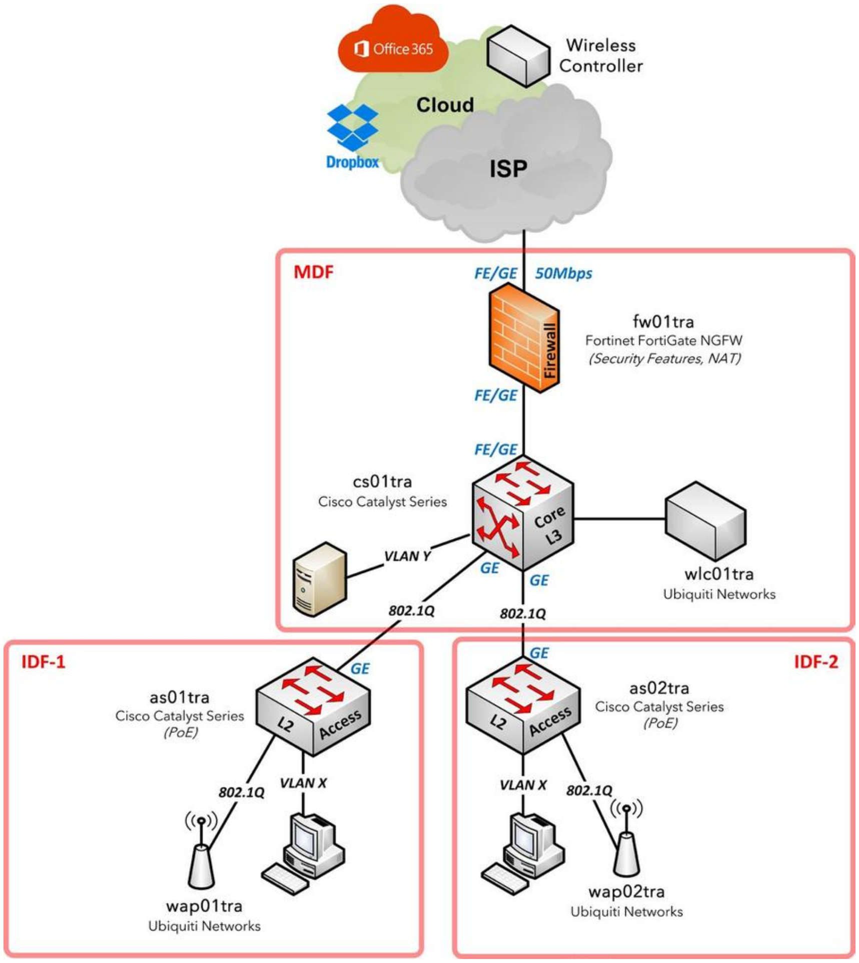
Core Switch (cs01) located in Tracy, CA (tra)

- **When to use**: this naming standard is ideal for networks located at a single location or sites located in different cities in the same state. This is typically used for small and SMB sized networks

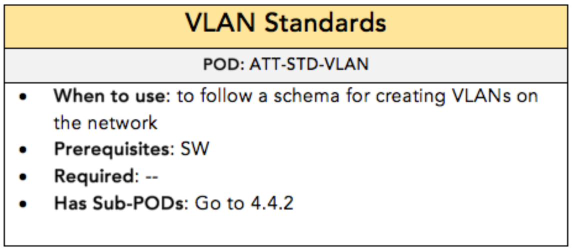
component-deviceID-location

- **Component**: the network device type
- **Device ID**: the network device number. This is important if there are multiple devices on the network
- **Location**: the location or city where the device is located

Therefore, this is how we can name each device in the topology:



For the VLAN standard, this has a prerequisite for the Switching POD which we already completed:

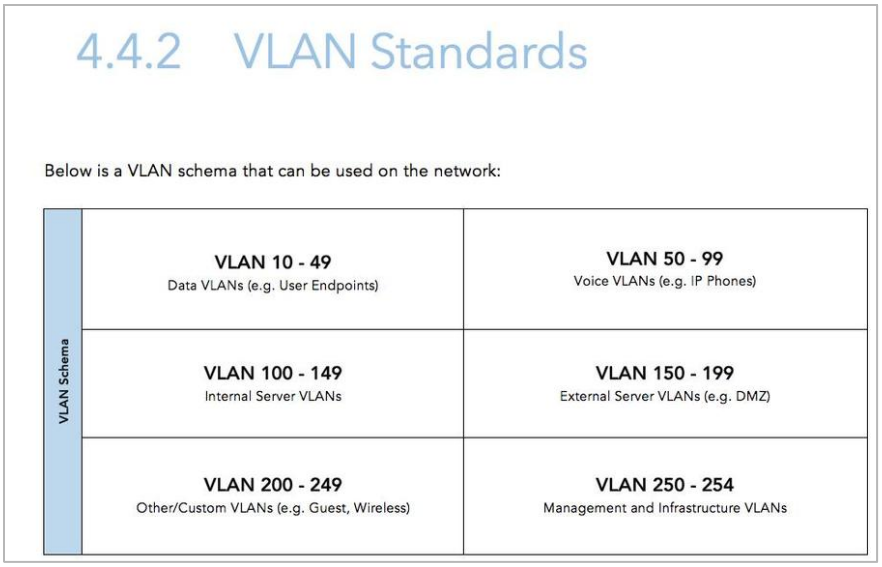


VLAN Standards

POD: ATT-STD-VLAN

- **When to use**: to follow a schema for creating VLANs on the network
- **Prerequisites**: SW
- **Required**: --
- **Has Sub-PODs**: Go to 4.4.2

When we go to section 4.4.2, you will see a VLAN schema that can be used and align with the addressing schema:



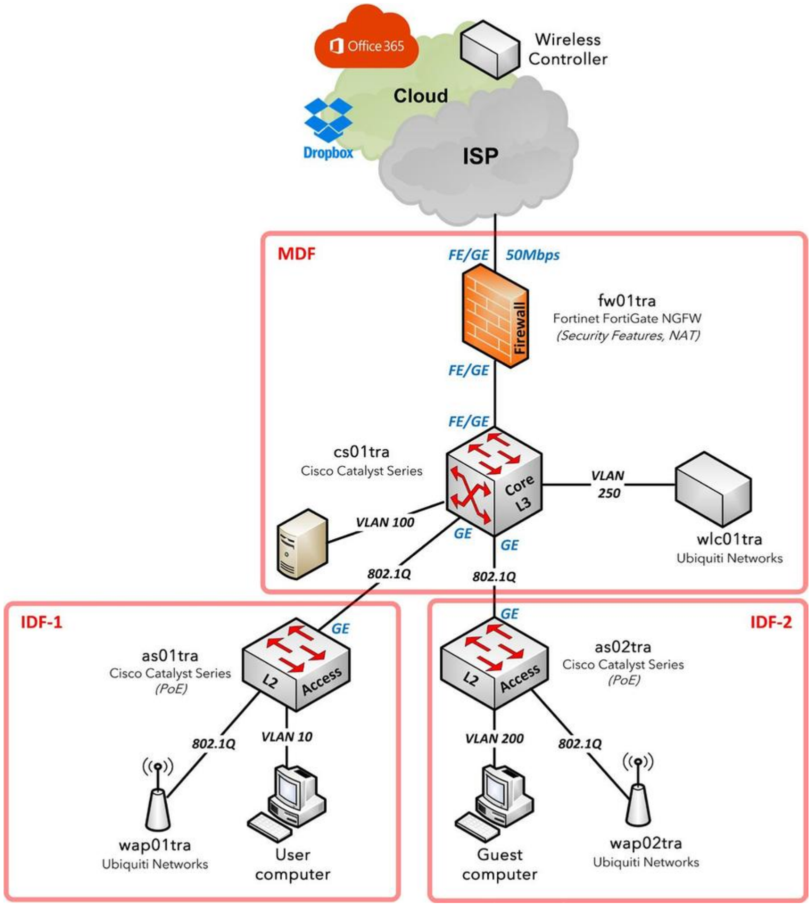
4.4.2 VLAN Standards

Below is a VLAN schema that can be used on the network:

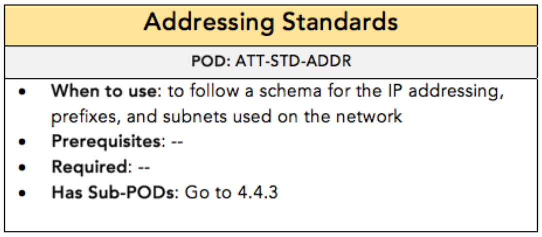
VLAN Schema	**VLAN 10 - 49** Data VLANs (e.g. User Endpoints)	**VLAN 50 - 99** Voice VLANs (e.g. IP Phones)
	VLAN 100 - 149 Internal Server VLANs	**VLAN 150 - 199** External Server VLANs (e.g. DMZ)
	VLAN 200 - 249 Other/Custom VLANs (e.g. Guest, Wireless)	**VLAN 250 - 254** Management and Infrastructure VLANs

For our customer design, we will use the following VLANs based on the networks that will be used:

- User - VLAN 10
- Guest - VLAN 200
- Server - VLAN 100
- Management - VLAN 250
- Transit - no VLAN required



Lastly, we can determine what addressing standard we want to follow which will align with our VLAN schema.

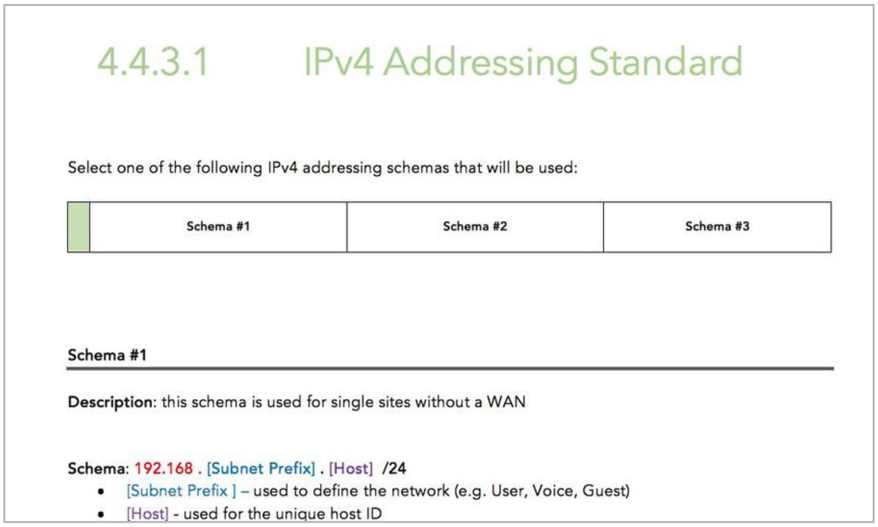


Addressing Standards

POD: ATT-STD-ADDR

- **When to use:** to follow a schema for the IP addressing, prefixes, and subnets used on the network
- **Prerequisites:** --
- **Required:** --
- **Has Sub-PODs:** Go to 4.4.3

This will present a standard for IPv4 and IPv6 addressing. In our customer design, we only require IPv4 addressing so we will continue on to section 4.4.3.1 to see what IPv4 addressing schemas we can consider:



4.4.3.1 IPv4 Addressing Standard

Select one of the following IPv4 addressing schemas that will be used:

🟩	**Schema #1**	**Schema #2**	**Schema #3**

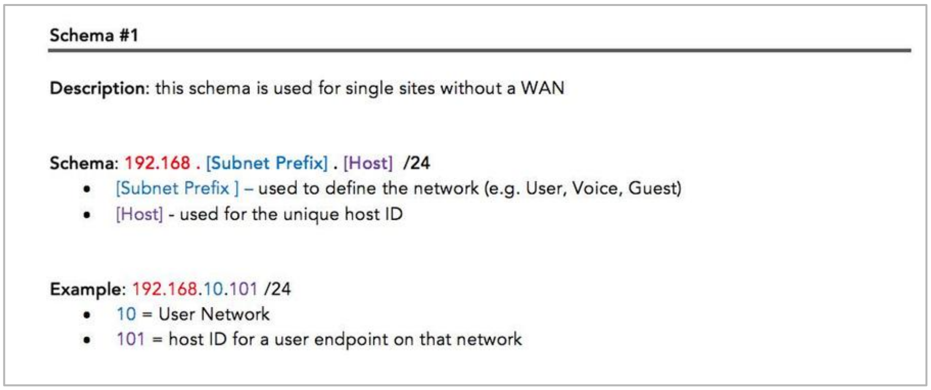
Schema #1

Description: this schema is used for single sites without a WAN

Schema: 192.168 . [Subnet Prefix] . [Host] /24

- [Subnet Prefix] – used to define the network (e.g. User, Voice, Guest)
- [Host] - used for the unique host ID

Here there are three different schemas that can be used for our internal network. For our customer design, we will use schema #1 which is typically aimed for single sites without a WAN.



Schema #1

Description: this schema is used for single sites without a WAN

Schema: 192.168 . [Subnet Prefix] . [Host] **/24**

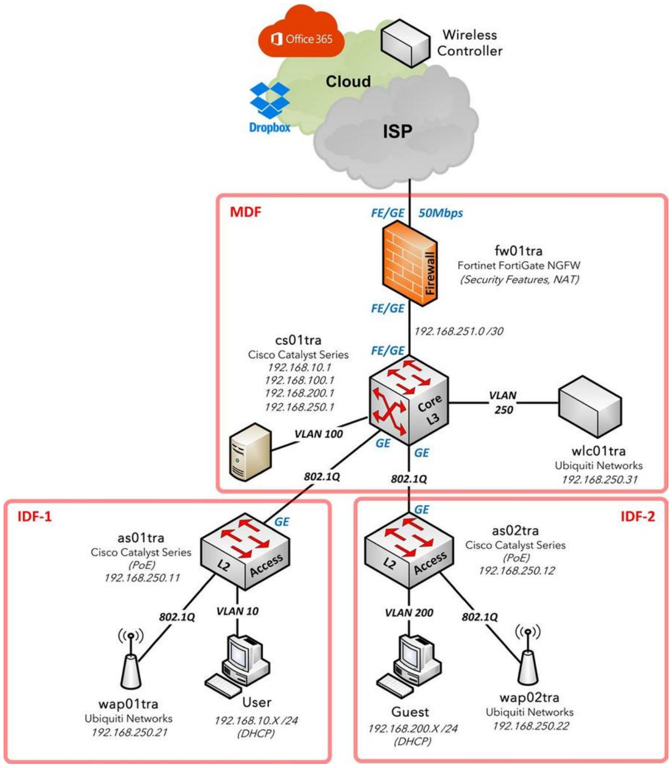
- [Subnet Prefix] – used to define the network (e.g. User, Voice, Guest)
- [Host] - used for the unique host ID

Example: 192.168.10.101 /24

- 10 = User Network
- 101 = host ID for a user endpoint on that network

This means the addressing (along with our VLAN schema and the networks that will be used) will be something like the following:

- User - VLAN 10 - 192.168.10.0 /24
- Guest - VLAN 200 - 192.168.200.0 /24
- Server - VLAN 100 - 192.168.100.0 /24
- Management - VLAN 250 - 192.168.250.0 /24
- Transit - no VLAN - 192.168.251.0 /30



We are now done with the customer design using the many PODs listed in the network design cookbook.

That is how you can use the design cookbook to build your own network designs based on the business requirements, technical objectives, to the engineer's professional preferences.

1. Frameworks

Select one (or more) of the following framework PODs that will be used in the design:

	Data Center	**LAN / Campus**	**WAN**
	Internet	**Service Provider**	

Data Center

POD: DC

- **When to use**: to build a network that is heavily focused on server endpoints
- **Prerequisites**: ATT-LOC
- **Required**: ATT-NET
- **Has Sub-PODs**: Go to 1.1

LAN / Campus

POD: LAN

- **When to use**: to build a network that is heavily focused on user endpoints
- **Prerequisites**: ATT-LOC
- **Required**: ATT-NET
- **Has Sub-PODs**: Go to 1.2

WAN

POD: WAN

- **When to use**: to build a network that will connect other LAN and/or Data Center networks together
- **Prerequisites**: LAN and/or DC, ATT-LOC
- **Required**: ATT-NET
- **Has Sub-PODs**: Go to 1.3

Internet

POD: INET

- **When to use**: to build a network that requires access to the Internet and/or provide Public facing services
- **Prerequisites**: LAN and/or DC
- **Required**: ATT-NET
- **Has Sub-PODs**: Go to 1.4

Service Provider

POD: SP

- **When to use**: to build a network that is heavily focused on connecting enterprise customer networks together. To build an Internet and/or WAN cloud used by customer networks.
- **Prerequisites**: --
- **Required**: VRT
- **Has Sub-PODs**: --

1.1 Data Center

Complete each of the design sections below for the solution.

Vendor Solutions

The hardware for the components in this framework consists of Data Center switches. Select one of the following vendors that will be used:

Hardware	**Cisco Switches** Cisco Nexus Series for Large DC networks Cisco Catalyst Series for Medium DC networks	**Juniper Switches** Juniper QFabric Series for Large DC networks Juniper EX Series for Medium and Large DC networks
	Arista Switches Arista 7000 Series for Medium and Large DC networks	

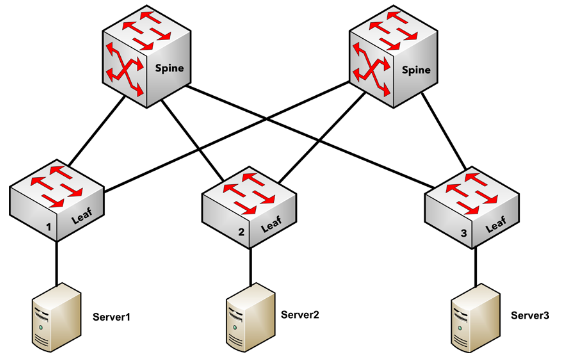
Main PODs

Select one of the following Data Center PODs that will be used:

	Spine-Leaf CLOS	**Traditional 1-Tier Topology**	**Traditional 2-Tier Topology**
	Converged Server Infrastructure		

Spine-Leaf CLOS

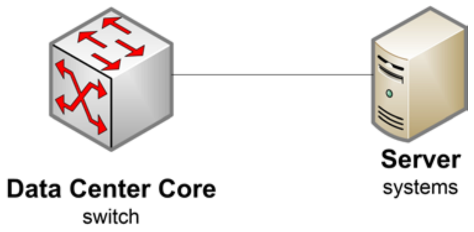
POD: DC-CLOS



- **When to use**: if there is a lot of server-to-server communication and the server endpoints are running similar functions
- **Prerequisites**: DC
- **Required**: DC-TR, SDN-DC or OVR-FP
- **Has Sub-PODs**: Go to 1.1.1
- **Components**: Spine Switch, Leaf Switch
- **Description**: this POD will consist of one (or more) leaf switches connecting to one (or more) spine switches. The server endpoints would be connected to the Leaf switches as shown in the picture above. Additional Ethernet switches can also be connected to the Leaf switches with server endpoints attached.

Traditional 1-Tier

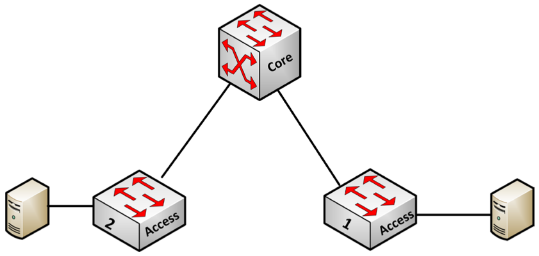
POD: DC-1T



- **When to use**: if the Data Center is heavily focused on server-to-user communication. And all server endpoints can be connected to a single network switch (fixed, stack, or chassis-based).
- **Prerequisites**: DC
- **Required**: SW
- **Has Sub-PODs**: Go to 1.1.2
- **Components**: Collapsed Core Switch
- **Description**: this POD will consist of one switch acting as the core switch that all server endpoints and network devices will be connected to. If there is a LAN core, it would be connected into the Core switch.

Traditional 2-Tier

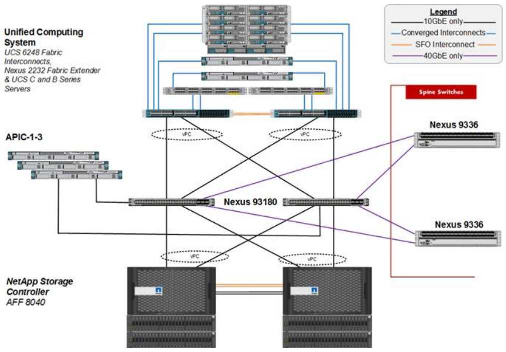
POD: DC-2T



- **When to use**: if the Data Center is heavily focused on machine-to-user communication and the server endpoints will be spread-out across several racks in the Data Center
- **Prerequisites**: DC
- **Required**: SW
- **Has Sub-PODs**: Go to 1.1.3
- **Components**: Core Switch, Access Switch
- **Description**: this POD will consist of one (or more) access switches connecting to one (or more) core switches. The server endpoints would be connected to the access switches. If there is a LAN core, it would be connected into the Core switch.

Converged Server Infrastructure

POD: DC-INF-C



- **When to use**: if you are looking for a validated pre-designed solution with unified computing, hypervisor, storage, and/or network switches composed of Cisco Data Center, VMware and NetApp (Storage) components.
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Spine Switches, Leaf Switches, Storage Array, Cisco UCS, APIC controllers
- **Description**: this POD will consist of a two-tier topology with a spine and leaf layer using Cisco Nexis switches. The storage devices (NetApp), UC devices (Cisco UCS), and the SDN controller (Cisco ACI) would plug into the Leaf switches in the topology.

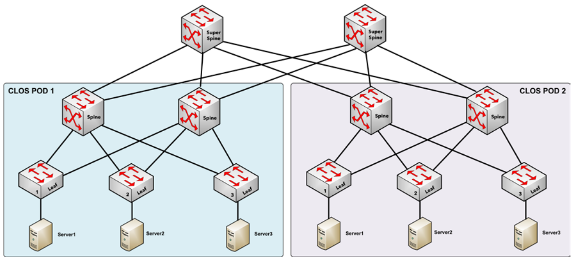
Add-On PODs

Select one (or more) of the following add-ons to include to the Data Center POD if needed:

Super Spine CLOS / Hyperscale	**Border CLOS**	**Top of Rack (ToR)**
Disaster Recovery	**Network Services**	**Custom**
Traditional Server Infrastructure	**Hyper-Converged Server Infrastructure**	**Management / OOB**

Super Spine CLOS / Hyperscale

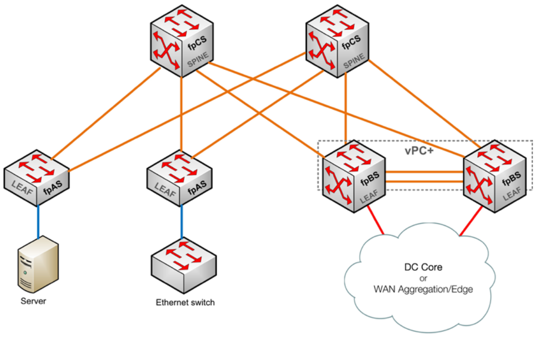
POD: DC-CLOS-SS



- **When to use**: if you require connecting several Spine-Leaf PODs together. And require connecting beyond 2500 servers.
- **Prerequisites**: DC-CLOS
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Super Spine Switch
- **Description**: this POD consists of one (or more) Spine-Leaf CLOS PODs connected to one (or more) Super Spine switches to provide a high number of server endpoints and forwarding performance.

Border CLOS

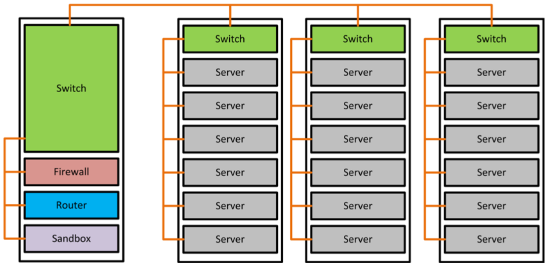
POD: DC-CLOS-B



- **When to use**: if you require connecting an Internet and/or WAN into the Data Center using a Spine-Leaf topology
- **Prerequisites**: DC-CLOS, INET and/or WAN
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Border Leaf Switch
- **Description**: this POD will connect to either the Super Spine or Spine switches in a CLOS topology.

Top of Rack

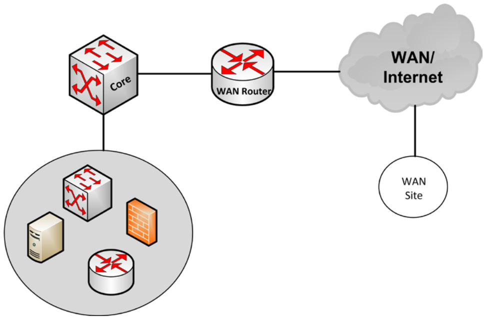
POD: DC-TR



- **When to use**: if multiple row of racks/cabinets exist in the Data Center and a 2-Tier topology will be deployed
- **Prerequisites**: DC-CLOS, DC-2T
- **Required**: --
- **Has Sub-PODs**: Go to 1.1.4
- **Components**: Access Switches
- **Description**: in this POD, you will determine if the access/leaf switches will be deployed in every rack, every other rack, or in a single rack.

Disaster Recovery (DR)

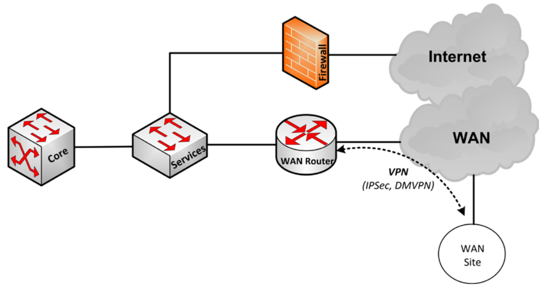
POD: DC-DR



- **When to use**: if you require having a backup location (or data center) that will host critical services and can be activated if a primary location (or data center) is no longer available.
- **Prerequisites**: DC-CLOS, DC-1T, or DC-2T
- **Required**: WAN and/or INET
- **Has Sub-PODs**: --
- **Components**: Core Switch, WAN/Internet Router
- **Description**: in this POD, the DR site can be a hot (all services running at full capacity), warm (partial services running at the site), or cold (requires turning on all services to be active) backup site for the network. All servers and network devices would be connected to a single Core switch. The DR location can be connected to either the Internet (using VPN or direct access) or into a L3 WAN as shown in the picture above.

Network Services

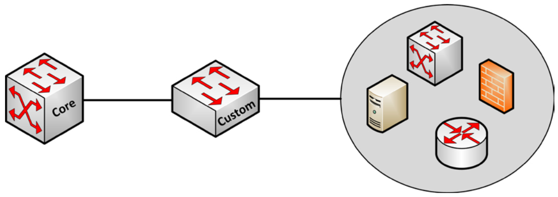
POD: DC-NS



- **When to use**: if you require a dedicated switch to be used for all network functions such as the Internet edge routers, firewalls, and/or WAN routers instead of being connected into the Core switch
- **Prerequisites**: DC-2T
- **Required**: --
- **Has Sub-PODs**: Go to 1.1.5
- **Components**: Network Services Switch
- **Description**: this POD consists of one (or more) dedicated switches that are reserved for network devices/solutions such as Internet edge routers, firewalls, and WAN routers. This switch would be connected to the core switch in the topology.

Custom

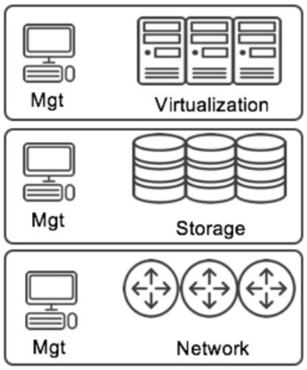
POD: DC-CUS



- **When to use**: if you require a dedicated switch to be used for a specific purpose and not connected directly into the Core switch
- **Prerequisites**: DC-2T
- **Required**: --
- **Has Sub-PODs**: Go to 1.1.5
- **Components**: Custom-purpose Switch
- **Description**: this POD consists of one (or more) dedicated switches that are reserved for a specific function to the topology (e.g. business partner, classroom, lab, etc.). This custom purpose switch would be connected to the core switch in the topology.

Traditional Server Infrastructure

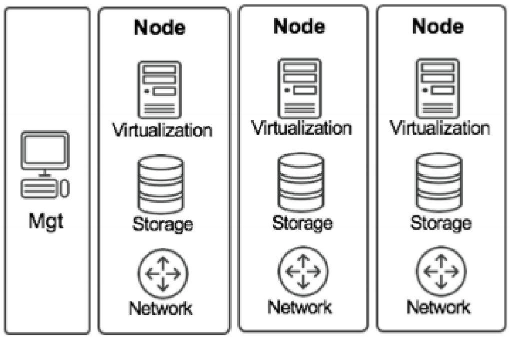
POD: DC-INF-T



- **When to use**: if you require deploying a standalone storage solution and computing solution within the data center
- **Prerequisites**: DC-CLOS, DC-1T, or DC-2T
- **Required**: SAN, COMP-UC (COMP-UC-T-UNF and/or COMP-UC-T-STD)
- **Has Sub-PODs**: --
- **Components**: Storage components, compute components, Data center switches (core, access)
- **Description**: this POD consists of separate storage components (e.g. technologies, switches and systems) and computing components (e.g. unified computing) connected within the data center.

Hyper-Converged Server Infrastructure

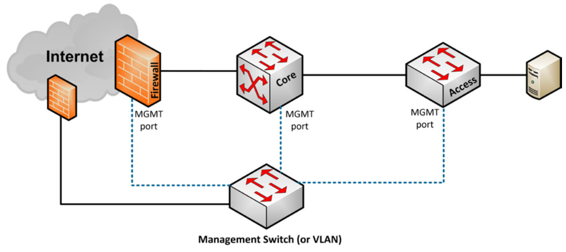
POD: DC-INF-HC



- **When to use**: if you require consolidating the computing, storage, and network resources to a single platform to lower the number of systems used in the data center with centralized management. HCI can also be used for VDI, Remote Offices, and development environments.
- **Prerequisites**: DC-CLOS, DC-1T, or DC-2T
- **Required**: COMP-UC (COMP-UC-HCI)
- **Has Sub-PODs**: --
- **Components**: HCI based systems, Data center switches (core, access)
- **Description**: in this POD the computing, storage, and network resources are virtualized on a single platform (called a node) which is connected within the data center with centralized management. Using HCI nodes will require greater performance on the data center switches.

Management / OOB

POD: DC-MGMT



- **When to use**: if you require a dedicated switch (or network) to be used for management purposes within the Data Center environment
- **Prerequisites**: DC-2T or DC-CLOS
- **Required**: --
- **Has Sub-PODs**: Go to 1.2.3
- **Components**: Management Switch
- **Description**: this POD consists of one (or more) dedicated switches that are reserved for network devices with management ports. This would likely be an isolated network used to provide remote administration if the Data Center becomes unavailable.

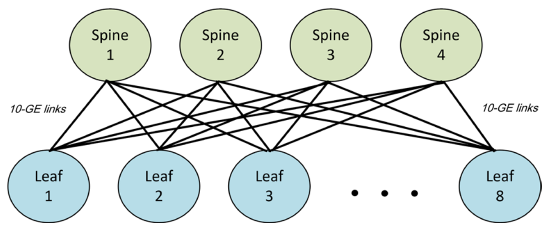
1.1.1 Spine-Leaf CLOS

Select one of the following Spine-Leaf CLOS PODs that will be used:

Small CLOS using 10GE	**Medium CLOS using 10GE**	**Large CLOS using 10GE**
Small CLOS using 40GE	**Medium CLOS using 40GE**	**Large CLOS using 40GE**
Hyperscale CLOS		

Small CLOS using 10GE

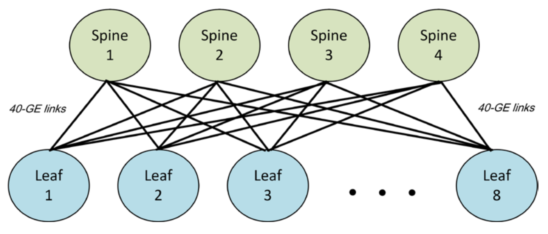
POD: DC-CLOS-S-10GE



- **When to use**: if you require support up to 32 10GE servers (or 320 1GE servers) within the CLOS using 10GE uplinks
- **Prerequisites**: DC-CLOS
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Spine Switch, Leaf Switch
- **Description**: in this POD, the CLOS consists of 8 leaf switches connected to 4 spine switches (each with a bandwidth capacity of 80Gbps) using 10GE connections. Each leaf switch can support 4 10GE servers (or 40 1GE servers).

Small CLOS using 40GE

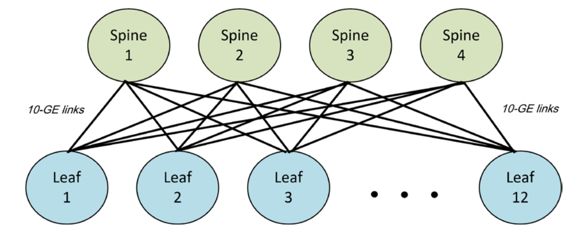
POD: DC-CLOS-S-40GE



- **When to use**: if you require support up to 128 10GE servers (or 1280 1GE servers) within the CLOS using 40GE uplinks
- **Prerequisites**: DC-CLOS
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Spine Switch, Leaf Switch
- **Description**: in this POD, the CLOS consists of 8 leaf switches connected to 4 spine switches (each with a bandwidth capacity of 320Gbps) using 40GE connections. Each leaf switch can support 16 10GE servers (or 160 1GE servers).

Medium CLOS using 10GE

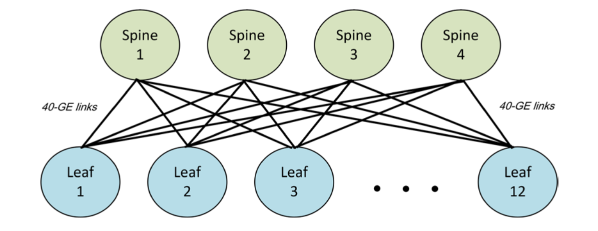
POD: DC-CLOS-M-10GE



- **When to use**: if you require support up to 48 10GE servers (or 480 1GE servers) within the CLOS using 10GE uplinks
- **Prerequisites**: DC-CLOS
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Spine Switch, Leaf Switch
- **Description**: in this POD, the CLOS consists of 12 leaf switches connected to 4 spine switches (each with a bandwidth capacity of 120Gbps) using 10GE connections. Each leaf switch can support 4 10GE servers (or 40 1GE servers).

Medium CLOS using 40GE

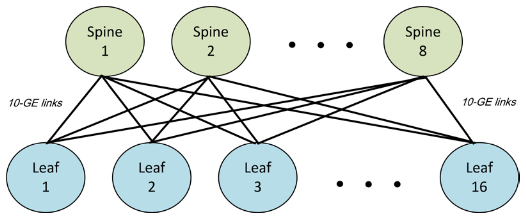
POD: DC-CLOS-M-40GE



- **When to use**: if you require support up to 192 10GE servers (or 1920 1GE servers) within the CLOS using 40GE uplinks
- **Prerequisites**: DC-CLOS
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Spine Switch, Leaf Switch
- **Description**: in this POD, the CLOS consists of 12 leaf switches connected to 4 spine switches (each with a bandwidth capacity of 480Gbps) using 40GE connections. Each leaf switch can support 16 10GE servers (or 160 1GE servers).

Large CLOS using 10GE

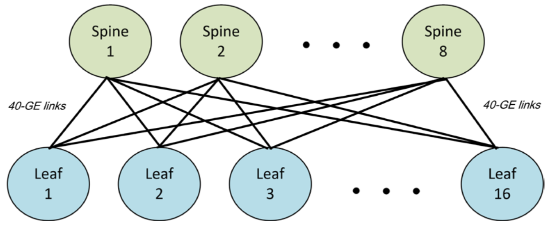
POD: DC-CLOS-L-10GE



- **When to use**: if you require support up to 128 10GE servers (or 1280 1GE servers) within the CLOS using 10GE uplinks
- **Prerequisites**: DC-CLOS
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Spine Switch, Leaf Switch
- **Description**: in this POD, the CLOS consists of 16 leaf switches connected to 8 spine switches (each with a bandwidth capacity of 160Gbps) using 10GE connections. Each leaf switch can support 8 10GE servers (or 80 1GE servers).

Large CLOS using 40GE

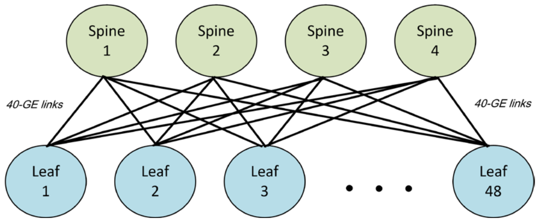
POD: DC-CLOS-L-40GE



- **When to use**: if you require support up to 512 10GE servers (or 5120 1GE servers) within the CLOS using 40GE uplinks
- **Prerequisites**: DC-CLOS
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Spine Switch, Leaf Switch
- **Description**: in this POD, the CLOS consists of 16 leaf switches connected to 8 spine switches (each with a bandwidth capacity of 640Gbps) using 40GE connections. Each leaf switch can support 32 10GE servers (or 320 1GE servers).

Hyperscale CLOS

POD: DC-CLOS-HS

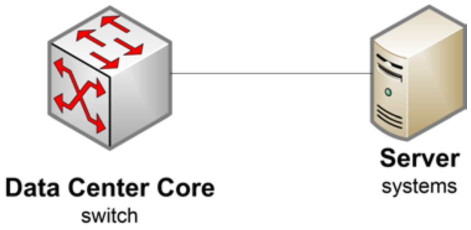
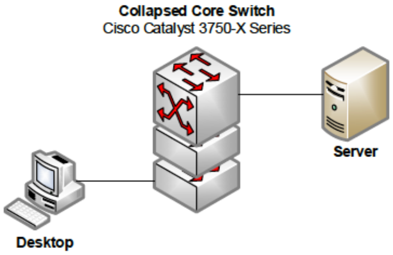


- **When to use**: if you require support up to 768 10GE servers (or 7680 1GE servers) within the CLOS using 40GE uplinks
- **Prerequisites**: DC-CLOS
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Spine Switch, Leaf Switch
- **Description**: in this POD, the CLOS consists of 48 leaf switches connected to 4 spine switches (each with a bandwidth capacity of 1.92Tbps) using 40GE connections. Each leaf switch can support 16 10GE servers (or 160 1GE servers).

1.1.2 Traditional 1-Tier Topology

Select one of the following Traditional 1-Tier PODs that will be used:

	Physical Topology	**Chassis/Stack Topology**

Physical Topology	Chassis/Stack Topology
POD: DC-1T-PHY	**POD**: DC-1T-C/S
	 Collapsed Core Switch Cisco Catalyst 3750-X Series Server Desktop
• **When to use**: if you require building a traditional Data Center using physical hardware for the core switch in the topology with a low port-capacity requirement • **Prerequisites**: DC-1T • **Required**: Fixed-based switch model • **Has Sub-PODs**: -- • **Description**: the collapsed core switch in this topology will consist of a fixed switch that isn't a chassis or stack-based switch that all server endpoints and network devices would be connected to	• **When to use**: if you require building a traditional Data Center using a single component but have a high port-capacity requirement • **Prerequisites**: DC-1T • **Required**: Chassis/Stack-based Switches • **Has Sub-PODs**: -- • **Description**: the collapsed core switch can consist of several switches stacked together or using a single chassis-based switch that all server endpoints and network devices would be connected to. This POD is ideal if you require a high port-capacity but still want to keep a 1-Tier Data Center topology.

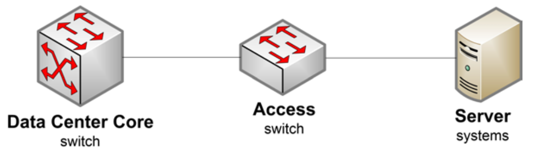
1.1.3 Traditional 2-Tier Topology

Select one of the following Traditional 2-Tier PODs that will be used:

Physical Topology	**Physical Topology with FHRP**	**Physical Topology with VPC**
Physical Topology with Chassis/Stack	**Virtual Topology**	**Unified Topology**
Unified Topology with VPC		

Physical Topology

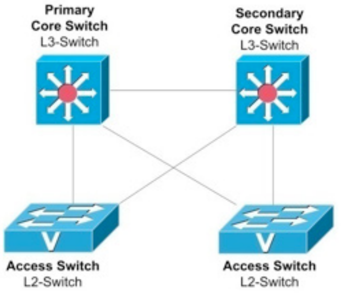
POD: DC-2T-PHY



- **When to use**: if you require building a traditional Data Center using physical hardware for each component in the topology
- **Prerequisites**: DC-2T
- **Required**: Fixed-based switch model
- **Has Sub-PODs**: --
- **Description**: all components in this topology will use fixed switches that isn't a chassis or stack-based switch that all server endpoints and network devices would be connected to. The access switches would be spread-out across several racks in the Data Center.

Physical Topology with FHRP

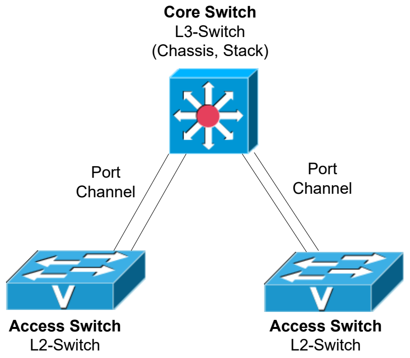
POD: DC-2T-PHY-FHRP



- **When to use**: if you require building a traditional Data Center using physical hardware with high-availability
- **Prerequisites**: DC-2T
- **Required**: Fixed-based switch model, REL-FHRP
- **Has Sub-PODs**: --
- **Description**: all components in this topology will use fixed switches. For high-availability, the topology will consist of redundant core switches. A link should be connected between the two Core switches especially if route summarization will be implemented for one (or more) networks within the Data Center. Each of the access switches (spread-out across several racks) would be connected to each of the core switches as shown in the picture above. The core switches will be configured to use a FHRP (e.g. HSRP or VRRP).

Physical Topology with Chassis/Stack

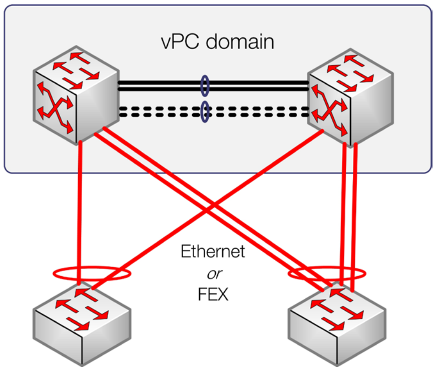
POD: DC-2T-PHY-C/S



- **When to use**: if you require building a traditional Data Center using physical hardware and want to achieve high-availability without using two physical core switches
- **Prerequisites**: DC-2T
- **Required**: Chassis/Stack Switches, OPS-PC
- **Has Sub-PODs**: --
- **Description**: in this POD, for high-availability, the core switch will consist of a chassis or stack-based switch. Each of the access switches (spread-out across several racks) would be connected to the core with multiple interfaces bundled together using a Port Channel. One connection would be plugged into a different line module (using chassis-based switch) or a different stack switch (using stack-based switch).

Physical Topology with VPC

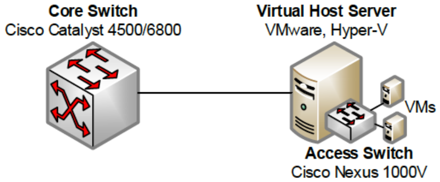
POD: DC-2T-PHY-VPC



- **When to use**: if you require building a traditional Data Center using physical hardware with high-availability without using a FHRP
- **Prerequisites**: DC-2T
- **Required**: Cisco Nexus series, OPS-CSCO-VPC
- **Has Sub-PODs**: --
- **Description**: in this POD, redundant core switches are configured to support Virtual Port Channels (vPC). This can allow a Port Channel to be implemented between two redundant Core switches to each access switch increasing the overall availability for the server endpoints on the switch. The access switch will think it is connected to a single Core switch in the topology.

Virtual Topology

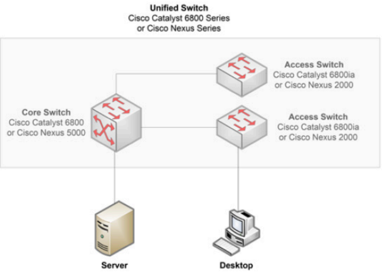
POD: DC-2T-VRT



- **When to use**: if you have many hypervisor hosts on the network with several virtual machines
- **Prerequisites**: DC-2T
- **Required**: Cisco Nexus 1000V
- **Has Sub-PODs**: --
- **Description**: in this POD, the access switches are virtualized within the Hypervisor host that the virtual servers are connected to. The virtual switches (and the Hypervisor host) would connect to the core switch in the topology.

Unified Topology

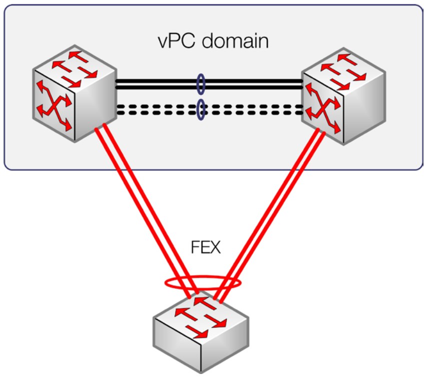
POD: DC-2T-UNF



- **When to use**: if your traditional Data Center components will exist in the same Data Center location which can be unified together to be managed as one logical switch
- **Prerequisites**: DC-2T
- **Required**: Cisco Nexus 5K/7K/6K (Core) + Nexus 2000 Series (Access)
- **Has Sub-PODs**: --
- **Description**: in this POD, the core and access switch components exist in the same room using unified-based hardware. The access switches (spread-out across several racks) would be treated as line modules on the core switch. As a result, the entire topology will be seen as one logical switch (or fabric) that can be managed from the core switch.

Unified Topology with VPC

POD: DC-2T-UNF-VPC



- **When to use**: if your traditional Data Center components will exist in the same Data Center location which can be unified together to be managed as one logical switch. And you require high-availability without using a FHRP
- **Prerequisites**: DC-2T
- **Required**: Cisco Nexus 5K/7K/6K (Core) + Nexus 2000 Series (Access), OPS-CSCO-VPC
- **Has Sub-PODs**: --
- **Description**: in this POD, redundant core switches and access switches exist in the same room using unified-based hardware. The access switches (spread-out across several racks) would be treated as line modules on the core switch. As a result, the entire topology will be seen as one logical switch that can be managed from the core switch. The core switches are configured to support Virtual Port Channels (vPC). Dual FEX connections exist between the access switches (using Nexus 2200 series) and the redundant VPC core switches (e.g. Nexus 5K/6K/7K series) increasing the overall availability for the server endpoints on the access switches.

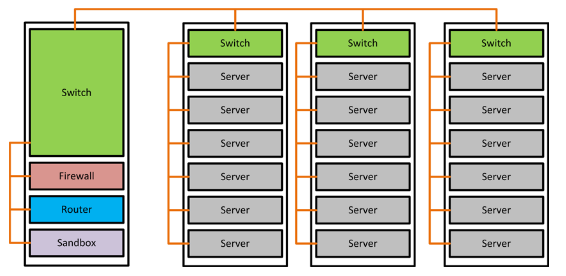
1.1.4 Top of Rack (ToR)

Select one of the following ways how the access (or leaf) switches will be deployed in the Data Center:

🟦	**Top of Rack (ToR)**	**End of Rack (EoR)**

Top of Rack (ToR)

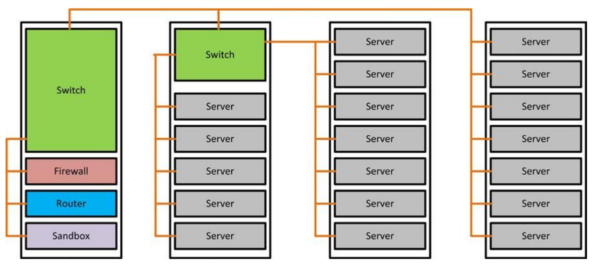
POD: DC-TR-TOR



- **When to use**: if you require placing an access switch at the top of each rack (or every other rack) to lower the amount of cabling across the Data Center
- **Prerequisites**: DC-TR
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: in this POD, each access switch is placed at the top of each rack (or every other rack) with servers in that rack connected to it directly.

End of Rack (EoR)

POD: DC-TR-EOR

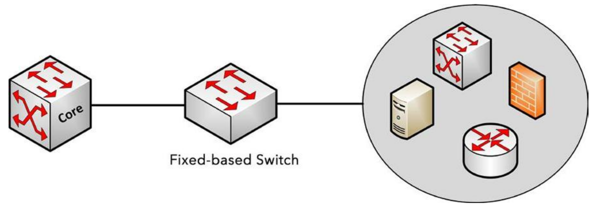
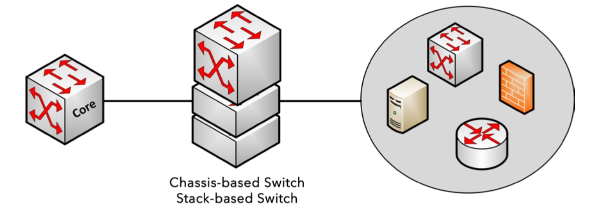


- **When to use**: if you require placing a single access switch (chassis/stack-based switch) at the end of each row of racks in the Data Center to lower the amount of access switches to manage.
- **Prerequisites**: DC-TR
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: in this POD, a single access switch is placed at the end of each row of racks with servers in that row connected to it directly.

1.1.5 Add-On Switches

Select one of the following Data Center add-on switch topologies (e.g. Network Services, Custom) that will be used:

	Physical Topology	**Chassis/Stack Topology**

Physical Topology	Chassis/Stack Topology
POD: DC-ADDON-PHY	**POD**: DC-ADDON-C/S
	
• **When to use**: if you require building the add-on switch using a fixed switch and require low port-capacity • **Prerequisites**: DC-NS, DC-CUS, DC-MGMT • **Required**: Fixed-based switches • **Has Sub-PODs**: -- • **Description**: the add-on switch in this topology will consist of a fixed switch that isn't a chassis or stack-based switch that all specified server endpoints (or network devices) would be connected to.	• **When to use**: if you require building the add-on switch using a single component but require a high port-capacity • **Prerequisites**: DC-NS, DC-CUS, DC-MGMT • **Required**: Chassis/Stack-based Switches • **Has Sub-PODs**: -- • **Description**: the add-on switch can consist of several switches stacked together or using a single chassis-based switch that all specified server endpoints (or network devices) would be connected to. This POD is ideal if you require a high port-capacity.

1.2 LAN / Campus

Complete each of the design sections below for the solution.

Vendor Solutions

The hardware for the components in this framework consists of LAN switches. Select one of the following vendors that will be used:

Hardware	**Cisco Switches** Cisco Catalyst Series for Large & Medium LAN Cisco Small Business for Small & SMB LAN Cisco Meraki for Small and SMB LAN	**Juniper Switches** Juniper EX Series for Medium and Large LAN

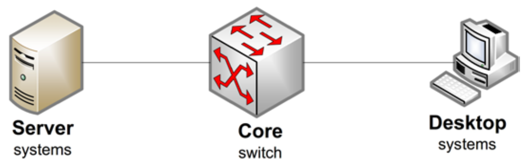
Main PODs

Select one of the following LAN PODs that will be used:

	Traditional 1-Tier Topology	**Traditional 2-Tier Topology**	**Traditional 3-Tier Topology**

Traditional 1-Tier LAN

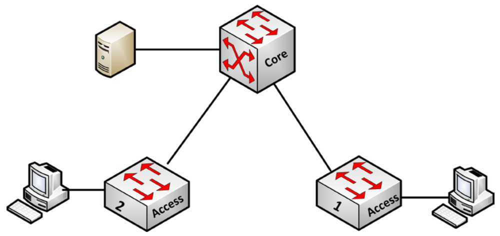
POD: LAN-1T



- **When to use**: if you have a LAN where all endpoints and network devices can be connected to a single switch located in a single room (e.g. Data Center)
- **Prerequisites**: LAN
- **Required**: SW
- **Has Sub-PODs**: Go to 1.2.1
- **Components**: Collapsed Core Switch
- **Description**: this POD will consist of one switch acting as the core switch that all endpoints and network devices will be connected to.

Traditional 2-Tier LAN

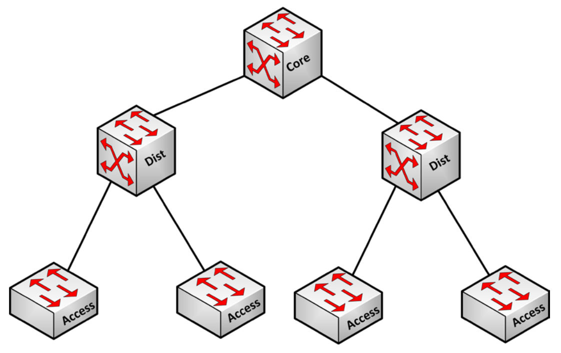
POD: LAN-2T



- **When to use**: if you have a LAN consisting over 48+ endpoints and network devices. Or if there are multiple wiring closets where equipment will be located. This is the most common and recommended topology that is used.
- **Prerequisites**: LAN
- **Required**: SW
- **Has Sub-PODs**: Go to 1.2.2
- **Components**: Core Switch, Access Switch
- **Description**: this POD will consist of one (or more) access switches connected to one (or more) core switches. The user endpoints would be connected to the access switches. The server endpoints (if any) would be connected directly into the core switch as shown in the picture above. If there is a Data Center core, it would be connected into the Core switch.

Traditional 3-Tier LAN

POD: LAN-3T



- **When to use**: if you have a large LAN with hundreds of endpoints spread out across multiple buildings with equipment located in several wiring closets
- **Prerequisites**: LAN
- **Required**: SW
- **Has Sub-PODs**: --
- **Components**: Core, Distribution, Access Switches
- **Description**: in this POD, you have a campus of several buildings. Each building will have wiring closets (IDF) with access switches that the user endpoints would be connected to. Each of the IDF rooms would connect to one (or more) distribution switches in the same building. There aggregation point. From there, each building distribution switch would be connected to a main building (or Data Center) consisting of one (or more) Core switches.

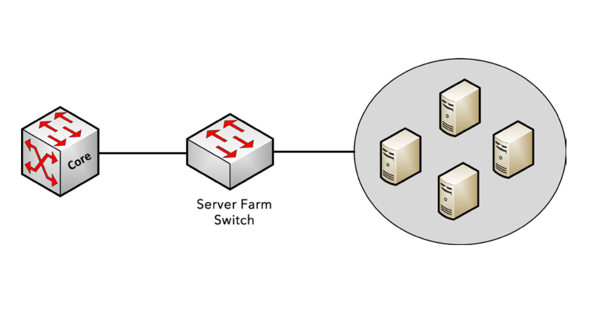
Add-On PODs

Select one (or more) of the following add-ons to include to the LAN POD if needed:

	Server Farm	**Network Services**	**Custom**

Server Farm

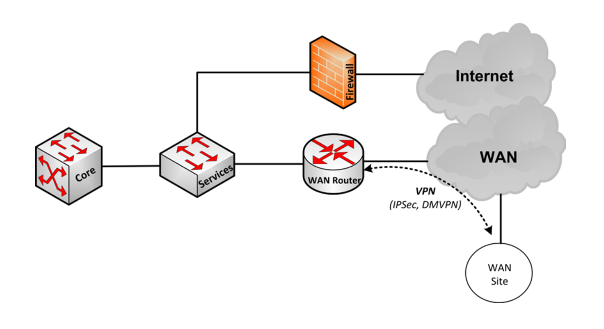
POD: LAN-SF



- **When to use**: if you require using a single switch for all server endpoints used on the LAN
- **Prerequisites**: LAN-2T or LAN-3T
- **Required**: --
- **Has Sub-PODs**: Go to 1.2.3
- **Components**: Server Farm Switch
- **Description**: this POD consists of one (or more) dedicated switches that are reserved for server endpoints. The server farm switch would be connected to one (or more) core switches in the topology.

Network Services

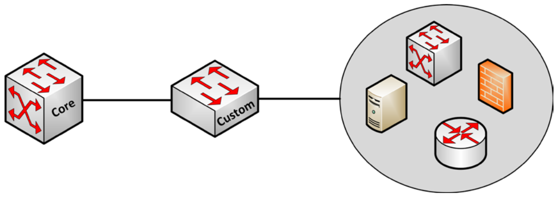
POD: LAN-NS



- **When to use**: if you require a dedicated switch to be used for all network functions such as the Internet edge routers, firewalls, and/or WAN routers instead of being connected into the Core switch
- **Prerequisites**: LAN-2T or LAN-3T
- **Required**: --
- **Has Sub-PODs**: Go to 1.2.3
- **Components**: Network Services Switch
- **Description**: this POD consists of one (or more) dedicated switches that are reserved for network devices/solutions such as Internet edge routers, firewalls, and WAN routers. This switch would be connected to one (or more) core switches in the topology.

Custom

POD: LAN-CUS



- **When to use**: if you require a dedicated switch to be used for a specific purpose and not connected directly into the Core switch
- **Prerequisites**: LAN-2T or LAN-3T
- **Required**: --
- **Has Sub-PODs**: Go to 1.2.3
- **Components**: Custom-purpose Switch
- **Description**: this POD consists of one (or more) dedicated switches that are reserved for a specific function to the topology (e.g. business partner, classroom, lab, etc.). This custom purpose switch would be connected to the core switch in the topology.

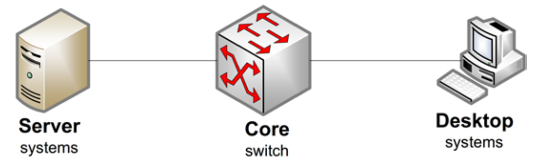
1.2.1 Traditional 1-Tier Topology

Select one of the following Traditional 1-Tier PODs that will be used:

	Physical Topology	**Chassis/Stack Topology**

Physical Topology

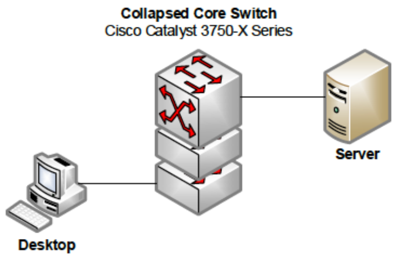
POD: LAN-1T-PHY



- **When to use**: if you require building a traditional LAN using physical hardware with a low port-capacity requirement
- **Prerequisites**: LAN-1T
- **Required**: Fixed-based switch model
- **Has Sub-PODs**: --
- **Description**: the collapsed core switch in this topology will consist of a fixed switch that isn't a chassis or stack-based switch that all endpoints and network devices would be connected to

Chassis/Stack Topology

POD: LAN-1T-C/S



- **When to use**: if you require building a traditional LAN using a single component but have a high port-capacity requirement
- **Prerequisites**: LAN-1T
- **Required**: Chassis/Stack-based Switches
- **Has Sub-PODs**: --
- **Description**: the collapsed core switch can consist of several switches stacked together or using a single chassis-based switch that all endpoints and network devices would be connected to. This POD is ideal if you require a high port-capacity but still want to keep a 1-Tier LAN topology.

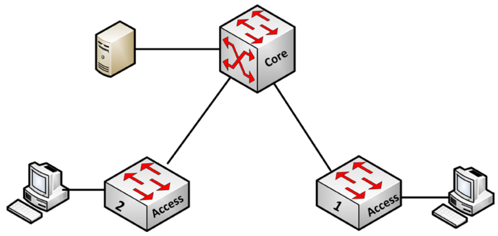
1.2.2 Traditional 2-Tier Topology

Select one of the following Traditional 2-Tier PODs that will be used:

	Physical Topology	**Physical Topology with FHRP**	**Physical Topology with VSS**
	Physical Topology with Chassis/Stack	**Unified Topology**	

Physical Topology

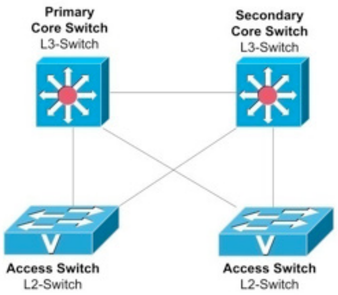
POD: LAN-2T-PHY



- **When to use**: if you require building a traditional LAN using fixed-based hardware for each component in the topology
- **Prerequisites**: LAN-2T
- **Required**: Fixed-based switch model
- **Has Sub-PODs**: --
- **Description**: all the components in this topology will consist of fixed-based switches that isn't a chassis or stack-based switch that all endpoints and network devices would be connected to. The access switches will exist in different wiring closets.

Physical Topology with FHRP

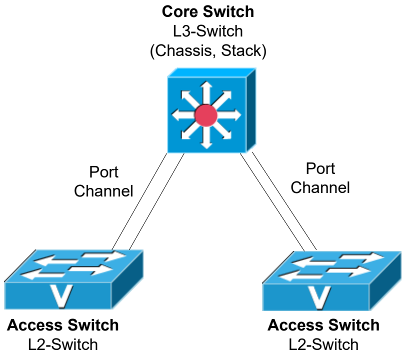
POD: LAN-2T-PHY-FHRP



- **When to use**: if you require building a traditional LAN using fixed-based hardware with high-availability
- **Prerequisites**: LAN-2T
- **Required**: Fixed-based switch model, REL-FHRP
- **Has Sub-PODs**: --
- **Description**: in this topology, all the components will use fixed-based switches. For high-availability, the topology will consist of redundant core switches. A link should be connected between the two Core switches especially if route summarization will be implemented for one (or more) networks within the LAN. Each of the access switches (located in different wiring closets) would be connected to each of the core switches as shown in the picture above. The core switches will be configured to use a FHRP (e.g. HSRP or VRRP).

Physical Topology with Chassis/Stack

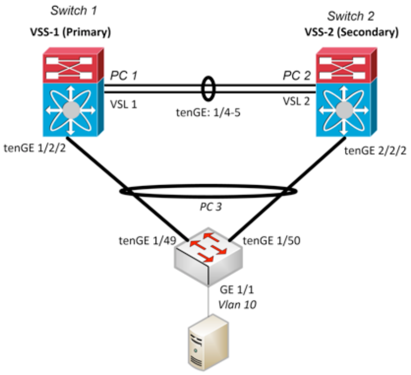
POD: LAN-2T-PHY-C/S



- **When to use**: if you require building a traditional LAN using physical hardware and want to achieve high-availability without using two physical core switches
- **Prerequisites**: LAN-2T
- **Required**: Chassis/Stack Switch, OPS-PC
- **Has Sub-PODs**: --
- **Description**: in this POD, for high-availability, the core switch will consist of a chassis or stack-based switch. Each of the access switches (located in different wiring closets) would be connected to the core with multiple interfaces bundled together using a Port Channel. One connection would be plugged into a different line module (using chassis-based switch) or to a different stack switch (using stack-based switch).

Physical Topology with VSS

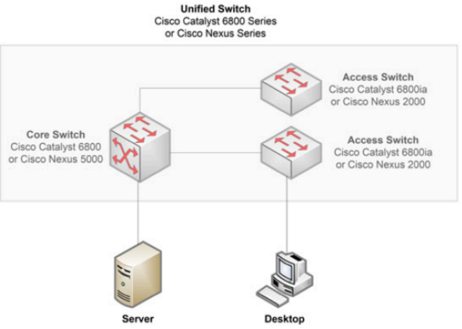
POD: LAN-2T-PHY-VSS



- **When to use**: if you require building a traditional LAN using physical hardware for high-availability without using FHRP. And the access switches will exist in different wiring closets.
- **Prerequisites**: LAN-2T
- **Required**: OPS-CSCO-VSS, OPS-PC, Hardware (Cisco Catalyst 6K series)
- **Has Sub-PODs**: --
- **Description**: in this topology, redundant core switches are clustered together to appear as one logical switch using VSS. A Port Channel would be implemented from the two redundant Core switches down to each access switch increasing its overall availability for the connected endpoints on the switch. The access switch will assume it is connected to a single Core switch in the topology.

Unified Topology

POD: LAN-2T-UNF



- **When to use**: if your traditional LAN components will exist in the same physical room which can be unified together to be managed as a single logical switch
- **Prerequisites**: LAN-2T
- **Required**: Cisco Catalyst 6800 (Core), 6800ia Series (Access)
- **Has Sub-PODs**: --
- **Description**: in this topology, the core and access components are in the same room using unified-based hardware. The access switches would be treated as line modules on the core switch meaning the entire topology will be seen as one logical switch (or fabric) that can be managed from the core switch.

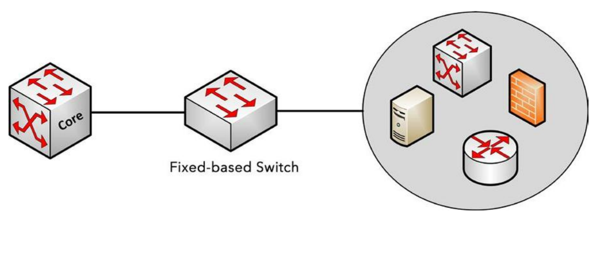
1.2.3 Add-On Switches

Select one of the following LAN add-on switch topologies (e.g. Server Farm, Network Services, Custom) that will be used:

	Physical Topology	**Chassis/Stack Topology**

Physical Topology

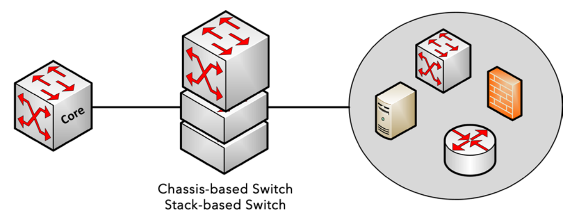
POD: LAN-ADDON-PHY



- **When to use**: if you require building the add-on switch using a fixed-based switch with low port-capacity
- **Prerequisites**: LAN-SF, LAN-NS, LAN-CUS
- **Required**: Fixed-based switches
- **Has Sub-PODs**: --
- **Description**: the add-on switch in this topology will consist of a fixed-based switch that isn't a chassis or stack-based switch that all server endpoints (or network devices) would be connected to.

Chassis/Stack Topology

POD: LAN-ADDON-C/S



- **When to use**: if you require building the add-on switch using a single component with high port-capacity
- **Prerequisites**: LAN-SF, LAN-NS, LAN-CUS
- **Required**: Chassis/Stack-based Switches
- **Has Sub-PODs**: --
- **Description**: the add-on switch can consist of several switches stacked together or using a single chassis-based switch that all server endpoints (or network devices) would be connected to. This POD is ideal if you require a high port-capacity with the add-on switch.

1.3 WAN

Complete each of the design sections below for the solution.

Vendor Solutions

The hardware for the components in this framework consists of routers. Select one of the following vendors that will be used:

Hardware	**Cisco Routers** Cisco ASR Series for Large WAN Cisco ISR Series for Medium to Large WAN Cisco Catalyst Series / Cisco Nexus Series	

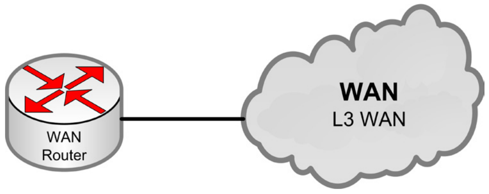
Main PODs

Select one of the following WAN PODs that will be used:

Single Router & WAN	**Single Router + Dual WAN**	**Dual Router + Single WAN**
Dual Router & WAN	**Edge Router/Firewall in Internet POD**	

Single Router & WAN

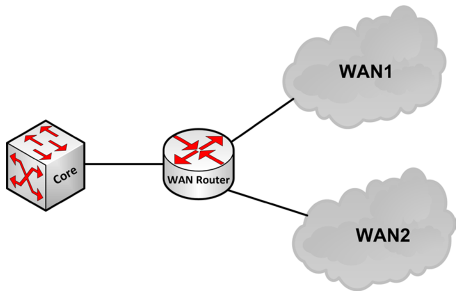
POD: WAN-SRW



- **When to use**: if you do not have high-availability (4-hours or longer downtime) requirements for providing access into the WAN
- **Prerequisites**: WAN
- **Required**: RT
- **Has Sub-PODs**: Go to 1.3.1
- **Components**: WAN router
- **Description**: in this POD, a single WAN router is connected to a single WAN provider and to either the Core switch (LAN/DC) or the Network Services switch in the topology.

Single Router + Dual WAN

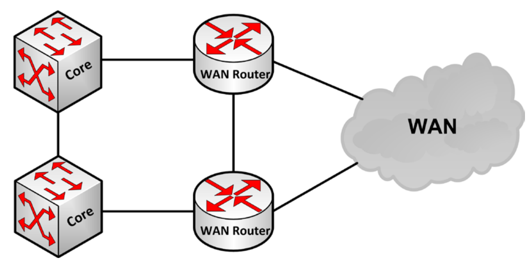
POD: WAN-SRDW



- **When to use**: if you require partial high-availability and have concerns that the WAN service provider is more likely to fail than the WAN router
- **Prerequisites**: WAN
- **Required**: RT
- **Has Sub-PODs**: Go to 1.3.2
- **Components**: WAN router
- **Description**: in this POD, a single WAN router is connected to two WAN providers. The WAN router is also connected down to either the Core switch (LAN/DC) or the Network Services switch in the topology.

Dual Router + Single WAN

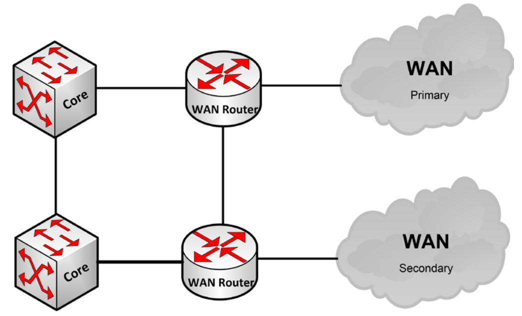
POD: WAN-DRSW



- **When to use**: if you require partial high-availability and have concerns that the hardware is more likely to fail than the WAN cloud (or its connection)
- **Prerequisites**: WAN
- **Required**: Routing
- **Has Sub-PODs**: Go to 1.3.1
- **Components**: WAN router
- **Description**: in this POD, dual WAN routers are connected to a single WAN provider. The WAN routers are also connected down to either the Core switch (LAN/DC) or the Network Services switch in the topology.

Dual Router & WAN

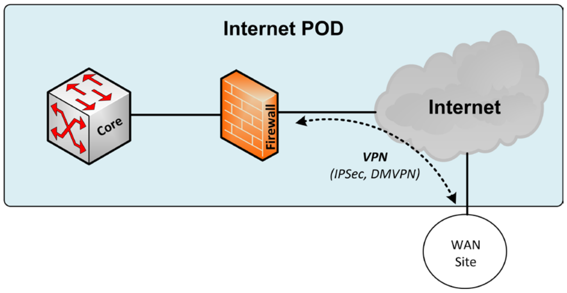
POD: WAN-DRW



- **When to use**: if you require full high-availability using redundant hardware and WAN clouds
- **Prerequisites**: WAN
- **Required**: RT
- **Has Sub-PODs**: Go to 1.3.2
- **Components**: WAN router
- **Description**: in this POD, dual WAN routers are connected to dual WAN providers as shown in the picture above. The WAN routers will also connect down to either the Core switch (LAN/DC) or the Network Services switch in the topology.

Edge Router/Firewall in Internet POD

POD: WAN-INET



- **When to use**: if you require using the existing Internet POD for connecting with other sites using IPsec VPN tunnels. This is common for small and SMB sized networks with sites connected to the Internet.
- **Prerequisites**: INET
- **Required**: SEC-NET-VPN-IPSEC1
- **Has Sub-PODs**: --
- **Components**: Edge router (or Firewall appliance)
- **Description**: this will use the existing Internet POD topology for providing WAN services with other sites located on the Internet using IPsec VPN tunnels.

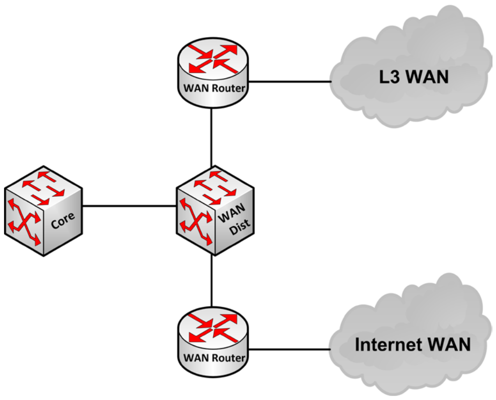
Add-On PODs

Select one (or more) of the following add-ons to include to the WAN POD if needed:

	WAN Distribution		

WAN Distribution

POD: WAN-DIST



- **When to use**: if you will have a large WAN with multiple WAN routers, clouds, and hundreds of remote sites. This is common for large networks with a large number of remote sites.
- **Prerequisites**: WAN-SRW, WAN-SRDW, WAN-DRSW, or WAN-DRW
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: WAN routers
- **Description**: in this POD, a WAN distribution switch/router is connected into the LAN/DC Core switch. It would also connect to one (or more) WAN routers and WAN clouds based on the requirements of the network as shown in the picture above.

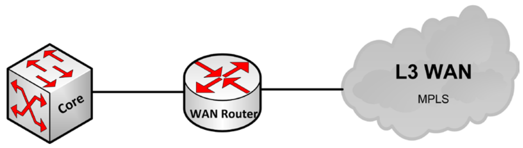
1.3.1 Single WAN

Select one of the following Single WAN PODs that will be used:

	Single L3 WAN	**Single L2 WAN**	**Single Internet WAN using VPN**
	Single Internet WAN using LISP		

Single L3 WAN

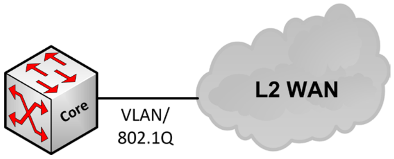
POD: WAN-S-L3WAN



- **When to use**: if you require the WAN router(s) to connect into a single L3 WAN to provide full mesh connectivity with all sites on the WAN
- **Prerequisites**: WAN-SRW or WAN-DRSW
- **Required**: RT and/or OVR-OTV
- **Has Sub-PODs**: --
- **Components**: WAN router(s), WAN cloud
- **Description**: in this POD, the WAN router(s) would be connected to a single L3 WAN cloud provider enabled for MPLS. The connection would be an Ethernet hand-off. Using a L3 WAN can provide direct access to any site connected to the WAN without going directly through another site (e.g. Main office or Data Center).

Single L2 WAN

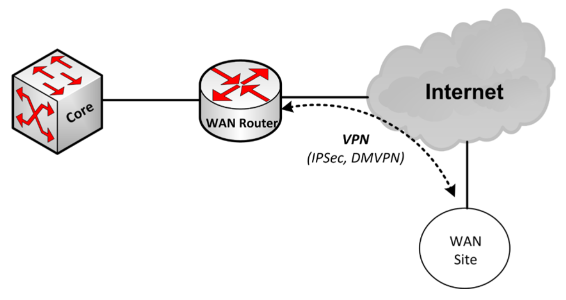
POD: WAN-S-L2WAN



- **When to use**: if you require the WAN router(s) to connect into a single L2 WAN to extend one (or more) VLANs with one (or more) sites on the WAN
- **Prerequisites**: WAN-SRW or WAN-DRSW
- **Required**: SW
- **Has Sub-PODs**: --
- **Components**: WAN router(s), WAN cloud
- **Description**: in this POD, the WAN router(s) would be connected to a single L2 WAN cloud provider enabled to support VLAN tagging. Using a L2 WAN can allow VLAN(s) to be used between sites connected to the WAN. As an alternative, the WAN router can be omitted and the L2 WAN using an Ethernet hand-off can be plugged directly into the LAN/DC Layer-3 Core switch as shown in the picture above.

Single Internet WAN using VPN

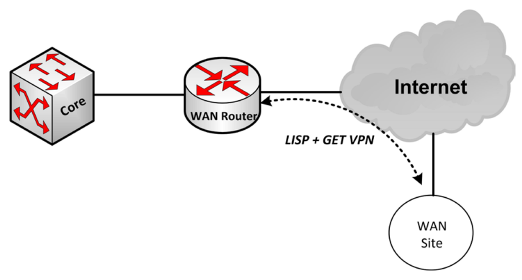
POD: WAN-S-IWAN-VPN



- **When to use**: if you require the WAN (or Internet edge) router(s) to connect into the Internet and use secure VPN tunnels to provide connectivity with other sites
- **Prerequisites**: INET, WAN-SRW or WAN-DRSW
- **Required**: RT, SEC-NET-VPN-SVPN
- **Has Sub-PODs**: --
- **Components**: WAN router(s), WAN cloud
- **Description**: in this POD, the WAN router would be connected to a single Internet provider with other sites connected to the Internet. The WAN router in the topology can either be (1) a dedicated WAN router(s) that is connected to the Internet. Or (2) use the existing Internet router (or firewall appliance) located in the Internet POD. The WAN router component would build secure VPN tunnels (e.g. IPsec, DMVPN) with other sites connected to the Internet.

Single Internet WAN using LISP

POD: WAN-S-IWAN-LISP



- **When to use**: if you require (1) the WAN (or Internet edge) router(s) to connect into the Internet. (2) You want to use LISP (for routing service) and GET VPN (for encryption services) to provide connectivity with other sites. And (3) the equipment will consist of Cisco routers.
- **Prerequisites**: INET, WAN-SRW or WAN-DRSW
- **Required**: OVR-LISP, SEC-NET-VPN-GETVPN
- **Has Sub-PODs**: --
- **Components**: WAN router(s), WAN cloud
- **Description**: in this POD, the WAN router would be connected to a single Internet provider with other sites connected to the Internet. The WAN router in the topology can either be (1) a dedicated WAN router(s) that is connected to the Internet. Or (2) use the existing Internet edge router located in the Internet POD. LISP would be used to provide routing services for connectivity between the sites. And GET VPN would be used with LISP to secure all data communication between the sites. The WAN router component must be a Cisco router device in the topology to support LISP and GET VPN services.

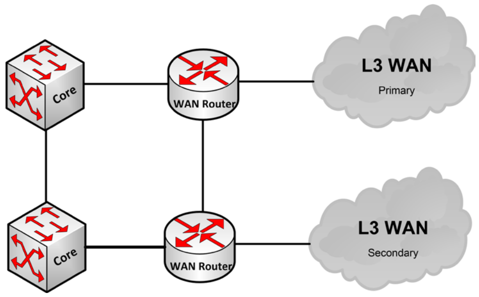
1.3.2 Dual WAN

Select one of the following Dual WAN PODs that will be used:

	Dual L3 WAN	**Dual L2 WAN**	**Dual Internet WAN**
	L3 WAN + Internet WAN using VPN	**L2 WAN + Internet WAN using VPN**	

Dual L3 WAN

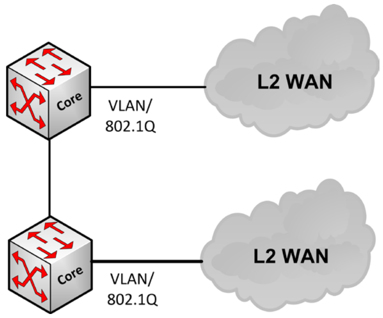
POD: WAN-D-L3WAN



- **When to use**: if you require the WAN router(s) to connect with two L3 WAN clouds to provide full mesh connectivity and redundancy with all sites on the WAN
- **Prerequisites**: WAN-SRDW or WAN-DRW
- **Required**: RT
- **Has Sub-PODs**: --
- **Components**: WAN router(s), WAN cloud
- **Description**: in this POD, the WAN router(s) would be connected to two L3 WAN (e.g. MPLS) cloud providers to provide cloud redundancy. Using a L3 WAN can provide direct access to any site connected to the WAN without going through another site (e.g. Main office or Data Center).

Dual L2 WAN

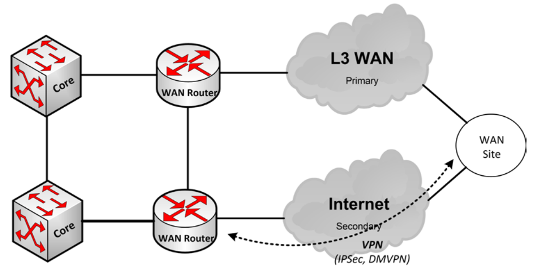
POD: WAN-D-L2WAN



- **When to use**: if you require the WAN router(s) to connect with two L2 WAN to extend one (or more) VLANs with one (or more) sites on the WAN. And to provide redundancy between the sites.
- **Prerequisites**: WAN-SRDW or WAN-DRW
- **Required**: SW
- **Has Sub-PODs**: --
- **Components**: WAN router(s), WAN cloud
- **Description**: in this POD, the WAN router(s) would be connected to two L2 WAN cloud providers enabled to support VLAN tagging and provide cloud redundancy. Using a L2 WAN can allow VLAN(s) to be used between sites connected to the WAN. As an alternative, the WAN routers can be omitted and the L2 WAN using an Ethernet hand-off can be plugged directly into the LAN/DC Layer-3 Core switches as shown in the picture above.

L3 WAN + Internet WAN using VPN

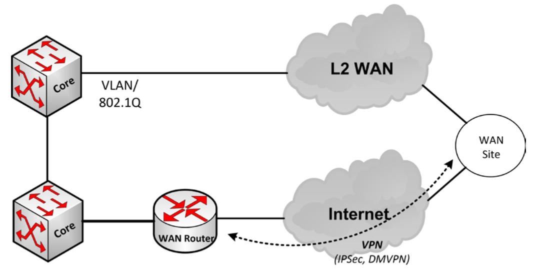
POD: WAN-D-L3WAN-IWAN-VPN



- **When to use**: if you require a L3 WAN, due to better SLA guarantees, but want an affordable redundant WAN cloud to be available if the primary WAN cloud fails
- **Prerequisites**: INET, WAN-SRDW or WAN-DRW
- **Required**: RT, SEC-NET-VPN-SVPN
- **Has Sub-PODs**: --
- **Components**: WAN router(s), WAN cloud
- **Description**: in this POD, the WAN router(s) would be connected to two different WAN clouds. The primary WAN would be a L3 WAN (e.g. MPLS) cloud provider. And the secondary WAN would be an Internet WAN configured to build secure VPN tunnels (e.g. IPsec, DMVPN) with other sites also connected to the Internet. The secondary WAN router in the topology can either be (1) a dedicated WAN router(s) that is connected to the Internet. Or (2) use the existing Internet edge router (or firewall appliance) located in the Internet POD. Both clouds can provide direct access to any site connected to the WAN without going through another site (e.g. Main office or Data Center). However, it requires a complex level of configuration to support this topology.

L2 WAN + Internet WAN using VPN

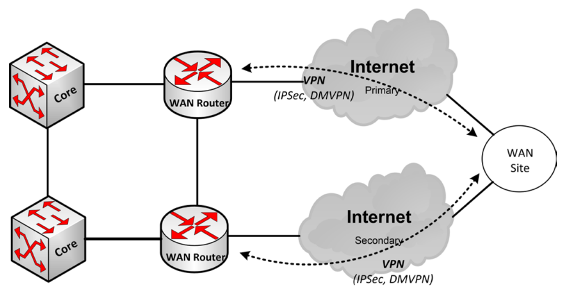
POD: WAN-D-L2WAN-IWAN-VPN



- **When to use**: if you require a L2 WAN, to support extending VLAN(s), but want an affordable redundant WAN cloud to be available if the primary WAN cloud fails
- **Prerequisites**: INET, WAN-SRDW or WAN-DRW
- **Required**: SW, RT, SEC-NET-VPN-SVPN
- **Has Sub-PODs**: --
- **Components**: WAN router(s), WAN cloud
- **Description**: in this POD, the WAN router(s) would be connected to two different WAN clouds. The primary WAN would be a L2 WAN (e.g. VPLS) cloud provider enabled to support VLAN tagging which would be plugged directly into the LAN/DC Layer-3 Core switch. And the secondary WAN would be an Internet WAN configured to build secure VPN tunnels (e.g. IPsec, DMVPN) with other sites also connected to the Internet. The secondary WAN router in the topology can either be (1) a dedicated WAN router(s) that is connected to the Internet. Or (2) use the existing Internet edge router (or firewall appliance) located in the Internet POD. Using this option requires a complex level of configuration to support this topology.

Dual Internet WAN using VPN

POD: WAN-D-IWAN



- **When to use**: if you require redundant WAN clouds, but want to use an affordable option for providing full mesh connectivity and redundancy with all sites on the WAN
- **Prerequisites**: INET, WAN-SRDW or WAN-DRW
- **Required**: RT, SEC-NET-VPN-SVPN
- **Has Sub-PODs**: --
- **Components**: WAN routers, WAN cloud(s)
- **Description**: in this POD, the WAN router(s) would be connected to two Internet providers with other sites also connected to the Internet. The two WAN router components in the topology can either be (1) a dedicated WAN router(s) that is connected to the Internet. Or (2) use the existing Internet edge router (or firewall appliance) located in the Internet POD. The WAN router components would build secure VPN tunnels (e.g. IPsec, DMVPN) with other sites connected to the Internet. Using this option requires a complex level of configuration to support this topology.

1.4 Internet

Complete each of the design sections below for the solution.

Vendor Solutions

The hardware for the components in this framework consists of Routers and/or Firewalls. Select one of the following vendors that will be used for the Internet edge routers (if applicable):

Hardware	**Cisco Routers** Cisco ASR Series for Large-sized network Cisco ISR Series for Medium to Large-sized network Cisco Meraki MX for Small & SMB-sized networks Cisco Catalyst Series / Cisco Nexus Series	

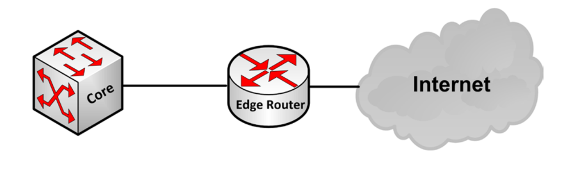
Main PODs

Select one of the following Internet PODs that will be used:

	Single Router & ISP	**Single Firewall & ISP**	**Single Router, Firewall, & ISP**
	Single Router + Dual ISP	**Single Firewall + Dual ISP**	**Single Router & Firewall + Dual ISP**
	Dual Router + Single ISP	**Dual Firewall + Single ISP**	**Dual Router & Firewall + Single ISP**
	Dual Router & ISP	**Dual Firewall & ISP**	**Dual Router, Firewall & ISP**

Single Router & ISP

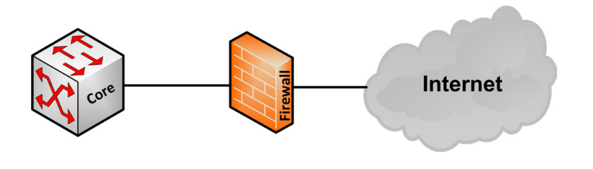
POD: INET-SRI



- **When to use**: if you require (1) a connection to the ISP using a T1 or ATM transport. (2) Basic firewall services (IP, Protocol, Port). And (3) do not have high-availability requirements for Internet services.
- **Prerequisites**: INET
- **Required**: RT, SEC-NET-FW (FW/ACL), NAT
- **Has Sub-PODs**: --
- **Components**: Edge router
- **Description**: in this POD, a single edge router is connected to a single ISP using one (or more) T1 or ATM connections. The edge router will be enabled for NAT and basic firewall services filtering based on the IP, protocol, and port number. It is also connected down to either the Core switch (LAN/DC) or the Network Services switch in the topology.

Single Firewall & ISP

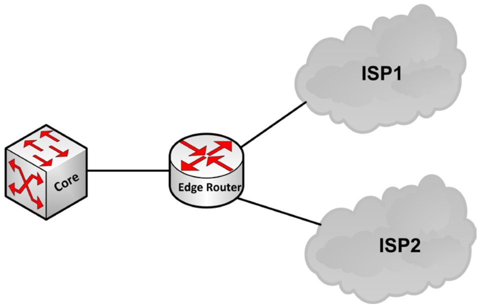
POD: INET-SFI



- **When to use**: if you require (1) a connection to the ISP using an Ethernet transport. (2) Advanced firewall services (NGFW, IPS, URL). And (3) do not have high-availability requirements for Internet services.
- **Prerequisites**: INET
- **Required**: RT, SEC-NET-FW (NGFW), NAT
- **Has Sub-PODs**: --
- **Components**: Firewall appliance
- **Description**: in this POD, a single next-generation firewall appliance is connected to a single ISP using an Ethernet connection. The firewall appliance will be enabled for NAT and advanced firewall services (e.g. application filtering, IPS). It is also connected down to either the Core switch (LAN/DC) or the Network Services switch in the topology.

Single Router + Dual ISP

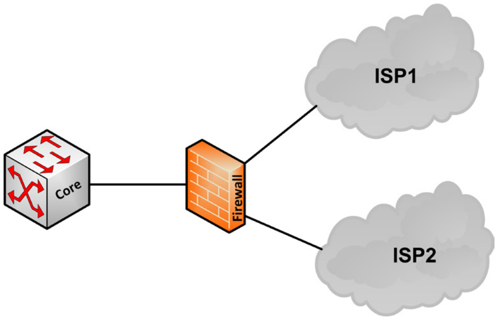
POD: INET-SRDI



- **When to use**: if you require (1) a connection to the ISP using a T1 or ATM transport. (2) Basic firewall services (IP, Protocol, Port). And (3) require partial high-availability with concerns that the ISP is more unreliable than a router failure.
- **Prerequisites**: INET
- **Required**: RT, SEC-NET-FW (FW/ACL), NAT
- **Has Sub-PODs**: --
- **Components**: Edge router
- **Description**: in this POD, a single edge router is connected to two (or more) ISP providers using T1 or ATM connections. The edge router will be enabled for NAT and basic firewall services filtering based on the IP, protocol, and port number. It is also connected down to either the Core switch (LAN/DC) or the Network Services switch in the topology.

Single Firewall + Dual ISP

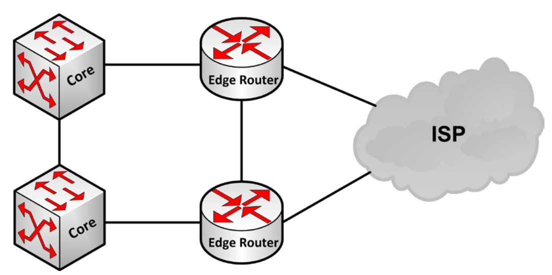
POD: INET-SFDI



- **When to use**: if you require (1) a connection to the ISP using an Ethernet transport. (2) Advanced firewall services (NGFW, IPS, URL). And (3) require partial high-availability with concerns that the ISP is more unreliable than a firewall failure.
- **Prerequisites**: INET
- **Required**: RT, SEC-NET-FW (NGFW), NAT
- **Has Sub-PODs**: --
- **Components**: Firewall appliance
- **Description**: in this POD, a single next-generation firewall appliance is connected to two (or more) ISP providers using Ethernet connections. The firewall appliance will be enabled for NAT and advanced firewall services (e.g. application filtering, IPS). It is also connected down to either the Core switch (LAN/DC) or the Network Services switch in the topology.

Dual Router + Single ISP

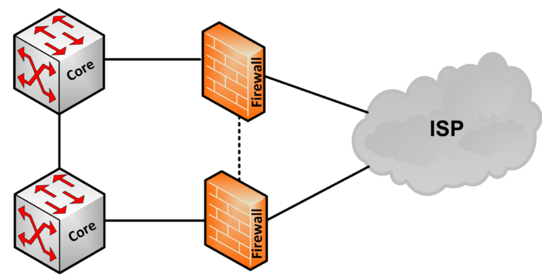
POD: INET-DRSI



- **When to use**: if you require (1) a connection to the ISP using a T1 or ATM transport. (2) Basic firewall services (IP, Protocol, Port). And (3) require partial high-availability with concerns that the hardware is more unreliable than a failure with the ISP cloud (or its connection).
- **Prerequisites**: INET
- **Required**: RT, SEC-NET-FW (FW/ACL), REL-FHRP (or RT), NAT
- **Has Sub-PODs**: --
- **Components**: Edge router
- **Description**: in this POD, two edge routers are connected to a single ISP using T1 or ATM connections. A link should be connected between the two edge routers. The edge router will be enabled for NAT and basic firewall services filtering based on the IP, protocol, and port number. It is also connected down to either the Core switch (LAN/DC) or the Network Services switch in the topology. Furthermore, the dual edge routers will be configured for FHRP or an IGP routing protocol (e.g. OSPF, EIGRP) if it is already used on the network.

Dual Firewall + Single ISP

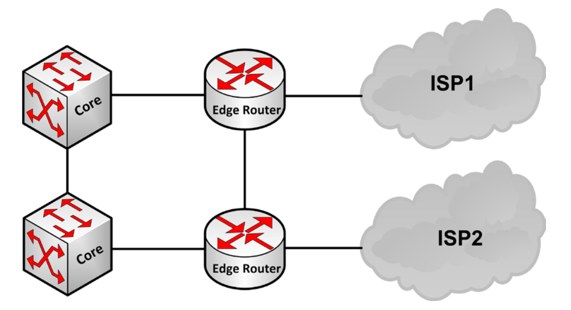
POD: INET-DFSI



- **When to use**: if you require (1) a connection to the ISP using an Ethernet transport. (2) Advanced firewall services (NGFW, IPS, URL). And (3) require partial high-availability with concerns that the hardware is more unreliable than a failure with the ISP cloud (or its connection).
- **Prerequisites**: INET
- **Required**: RT, SEC-NET-FW (NGFW), NAT
- **Has Sub-PODs**: --
- **Components**: Firewall appliance
- **Description**: in this POD, two next-generation firewalls (likely in an Active/Active configuration) are connected to a single ISP using Ethernet connections. The firewall appliance will be enabled for NAT and advanced firewall services (e.g. application filtering, IPS). It is also connected down to either the Core switch (LAN/DC) or the Network Services switch in the topology.

Dual Router & ISP

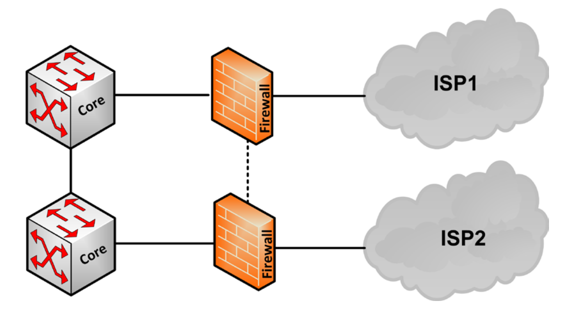
POD: INET-DRI



- **When to use**: if you require (1) a connection to the ISP using a T1 or ATM transport. (2) Basic firewall services (IP, Protocol, Port). And (3) require full high-availability using redundant hardware and ISP clouds.
- **Prerequisites**: INET
- **Required**: RT, SEC-NET-FW (FW/ACL), REL-FHRP (or RT), NAT
- **Has Sub-PODs**: --
- **Components**: Edge router
- **Description**: in this POD, two edge routers are connected to two (or more) ISP providers using T1 or ATM connections. A link should be connected between the two edge routers. The edge routers will be enabled for NAT and basic firewall services filtering based on the IP, protocol, and port number. It is also connected down to either the Core switch (LAN/DC) or the Network Services switch in the topology. Furthermore, the dual edge routers will be configured for FHRP or an IGP routing protocol (e.g. OSPF, EIGRP) if it is already used on the network.

Dual Firewall & ISP

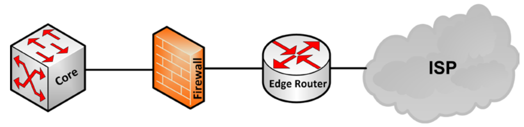
POD: INET-DFI



- **When to use**: if you require (1) a connection to the ISP using an Ethernet transport. (2) Advanced firewall services (NGFW, IPS, URL). And (3) require full high-availability using redundant hardware and ISP clouds.
- **Prerequisites**: INET
- **Required**: RT, SEC-NET-FW (NGFW), NAT
- **Has Sub-PODs**: --
- **Components**: Firewall appliance
- **Description**: in this POD, two next-generation firewalls (in an Active/Active configuration) are connected to two (or more) ISP providers using Ethernet connections. The firewall appliance will be enabled for NAT and advanced firewall services (e.g. application filtering, IPS). It is also connected down to either the Core switch (LAN/DC) or the Network Services switch in the topology.

Single Router, Firewall & ISP

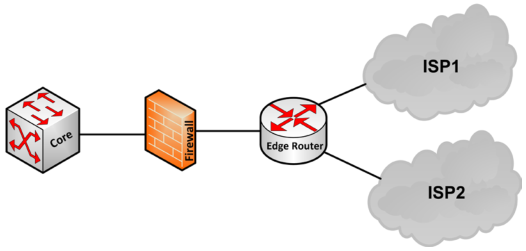
POD: INET-SRFI



- **When to use**: if you require (1) a connection to the ISP using a T1 or ATM transport. (2) Advanced firewall services (NGFW, IPS, URL). And (3) do not have high-availability requirements for Internet services.
- **Prerequisites**: INET
- **Required**: RT, SEC-NET-FW (NGFW), NAT
- **Has Sub-PODs**: --
- **Components**: Edge router, Firewall appliance
- **Description**: in this POD, a single edge router is directly connected to a single ISP using T1 or ATM connections. Connected in-line between the edge router and the LAN/DC is a firewall appliance enabled for NAT and advanced firewall services (e.g. application filtering, IPS). The firewall appliance would be connected down to either the Core switch (LAN/DC) or the Network Services switch in the topology.

Single Router & Firewall + Dual ISP

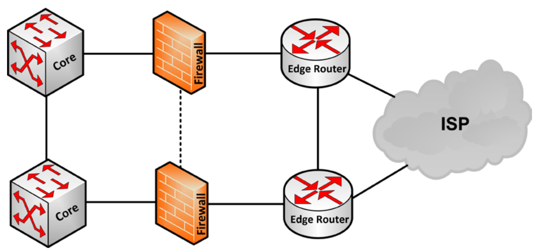
POD: INET-SRFDI



- **When to use**: if you require (1) a connection to the ISP using a T1 or ATM transport. (2) Advanced firewall services (NGFW, IPS, URL). And (3) require partial high-availability with concerns that the ISP is more unreliable than a hardware failure.
- **Prerequisites**: INET
- **Required**: RT, SEC-NET-FW (NGFW), NAT
- **Has Sub-PODs**: --
- **Components**: Edge router, Firewall appliance
- **Description**: in this POD, a single edge router is directly connected to two (or more) ISP providers using T1 or ATM connections. Connected in-line between the edge router and the LAN/DC is a firewall appliance enabled for NAT and advanced firewall services (e.g. application filtering, IPS). The firewall appliance would be connected down to either the Core switch (LAN/DC) or the Network Services switch in the topology.

Dual Router & Firewall + Single ISP

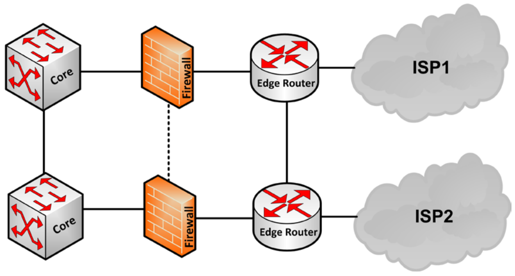
POD: INET-DRFSI



- **When to use**: if you require (1) a connection to the ISP using a T1 or ATM transport. (2) Advanced firewall services (NGFW, IPS, URL). And (3) require partial high-availability with concerns that the hardware is more unreliable than a failure with the ISP cloud (or its connection).
- **Prerequisites**: INET
- **Required**: RT, SEC-NET-FW (NGFW), FHRP (or RT), NAT
- **Has Sub-PODs**: --
- **Components**: Edge router, Firewall appliance
- **Description**: in this POD, dual edge routers are directly connected to a single ISP using T1 or ATM connections. A link should be connected between the two edge routers. Connected in-line between the edge routers and the LAN/DC are redundant firewall appliances enabled for NAT and advanced firewall services (e.g. application filtering, IPS). The firewall appliances would be connected down to either the Core switch (LAN/DC) or the Network Services switch in the topology. Furthermore, the dual edge routers will be configured for FHRP or an IGP routing protocol (e.g. OSPF, EIGRP) with the firewall appliance if it will be used in the environment.

Dual Router, Firewall, & ISP

POD: INET-DRFI



- **When to use**: if you require (1) a connection to the ISP using a T1 or ATM transport. (2) Advanced firewall services (NGFW, IPS, URL). And (3) require full high-availability using redundant hardware and ISP clouds.
- **Prerequisites**: INET
- **Required**: RT, SEC-NET-FW (NGFW), FHRP (or RT), NAT
- **Has Sub-PODs**: --
- **Components**: Edge router, Firewall appliance
- **Description**: in this POD, dual edge routers are directly connected to two (or more) ISP providers using T1 or ATM connections. A link should be connected between the two edge routers. Connected in-line between the edge routers and the LAN/DC are redundant firewall appliances enabled for NAT and advanced firewall services (e.g. application filtering, IPS). The firewall appliances would be connected down to either the Core switch (LAN/DC) or the Network Services switch in the topology. Furthermore, the dual edge routers will be configured for FHRP or an IGP routing protocol (e.g. OSPF, EIGRP) with the firewall appliance if it will be used in the environment.

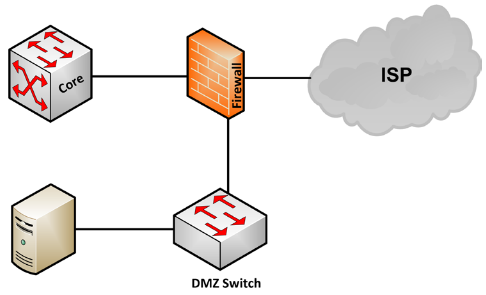
Add-On PODs

Select one (or more) of the following add-ons to include to the Internet POD if needed:

🟨	**DMZ**	**Custom (Internal)**	**Custom (External)**

DMZ

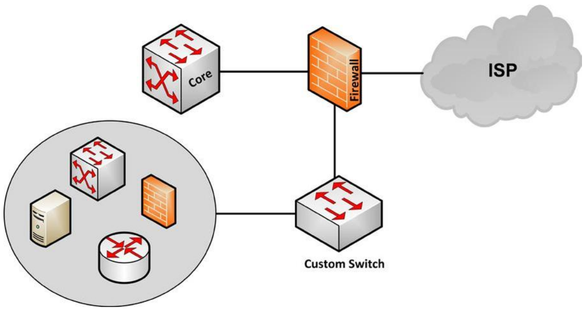
POD: INET-DMZ



- **When to use**: if you require a dedicated network for public facing servers and don't want servers located on the LAN/DC to be accessed directly from the Internet.
- **Prerequisites**: INET-*
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: DMZ switch
- **Description**: in this POD, a dedicated switch is used for Public facing servers. The DMZ switch will typically be plugged into a dedicated port on the firewall appliance as shown in the picture above.

Custom (Internal)

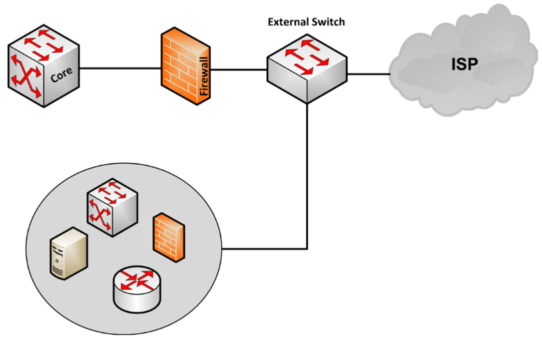
POD: INET-CUS1



- **When to use**: if you require a dedicated network to be used for a specific purpose within the Internet POD
- **Prerequisites**: INET-*
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Custom-purpose Switch
- **Description**: this POD can consist of a dedicated switch, router, and/or firewall that is reserved for a specific function to the topology (e.g. business partner). This custom purpose network would be connected into a dedicated port on the firewall appliance as shown in the picture above.

Custom (External)

POD: INET-CUS2



- **When to use**: if you require a dedicated network to be connected externally within the Internet POD
- **Prerequisites**: INET-*
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: External Switch, External Network
- **Description**: in this POD, an external switch is used between the ISP, the main Internet POD, and a separate managed network as shown in the picture above. This POD is typically used if another business wants to utilize the same Internet connection and will be managing their own network devices. This POD can also be used if you require a separate external network that isn't directly connected with the main production network based on a specific security requirement.

2. Solutions

Select one (or more) of the following solution PODs that will be used in the design:

Collaboration (Voice, Video)	**Computing**	**Load Balancing**
Network Management	**Optimization**	**Security**
Software Defined Networks (SDN)	**Storage**	**Wireless**

Collaboration (Voice / Video)

POD: COL

- **When to use**: if you require implementing voice or video services on the network
- **Prerequisites**: LAN
- **Required**: --
- **Has Sub-PODs**: Go to 2.1

Computing

POD: COMP

- **When to use**: if you require using cloud services and/or building a computing system (traditional, HCI)
- **Prerequisites**: LAN and/or DC
- **Required**: --
- **Has Sub-PODs**: Go to 2.2

Load Balancing

POD: LB

- **When to use**: to provide distribution of traffic across a group of servers (local) or data center sites (global)
- **Prerequisites**: DC, INET
- **Required**: --
- **Has Sub-PODs**: Go to 2.3

Network Management

POD: NM

- **When to use**: if you want to monitor the performance and faults located on the network or any of its devices
- **Prerequisites**: LAN and/or DC
- **Required**: --
- **Has Sub-PODs**: Go to 2.4

Optimization

POD: OPT

- **When to use**: if you want to increase performance for user endpoints across a slow (high latency) network (e.g. WAN)
- **Prerequisites**: WAN
- **Required**: --
- **Has Sub-PODs**: Go to 2.5

Security

POD: SEC

- **When to use**: if you want to implement network, application, endpoint, and/or data security for your environment. Strongly recommended for selection. Or if the business has regulatory/compliancy requirements.
- **Prerequisites**: INET, LAN and/or DC
- **Required**: --
- **Has Sub-PODs**: Go to 2.6

Software Defined Networks (SDN)

POD: SDN

- **When to use**: if there is a lot of machine-to-machine communication running similar functions and you want to manage the entire network from a centralized controller
- **Prerequisites**: DC, WAN
- **Required**: --
- **Has Sub-PODs**: Go to 2.7

Storage

POD: SAN

- **When to use**: if you require deploying a storage system in the data center that will store server data or where servers will boot from
- **Prerequisites**: DC
- **Required**: --
- **Has Sub-PODs**: Go to 2.8

Wireless

POD: WIFI

- **When to use**: if you require implementing wireless capabilities that user endpoints can use for accessing the network
- **Prerequisites**: LAN
- **Required**: --
- **Has Sub-PODs**: Go to 2.9

2.1 Collaboration

Select one (or more) of the following Collaboration PODs that will be used in the design:

Voice / Unified Communications	**Messaging**	**Call Center**
Conferencing	**Presence**	**Video**

Voice / Unified Communications

POD: COL-VOICE

- **When to use**: if you require providing voice services to support inbound and outbound calling
- **Prerequisites**: COL
- **Required**: QOS, MCAST, OPS-NTP
- **Has Sub-PODs**: Go to 2.1.1

Messaging

POD: COL-MSG

- **When to use**: if you require voicemail and Auto Attendant services with the voice solution
- **Prerequisites**: COL-VOICE
- **Required**: --
- **Has Sub-PODs**: Go to 2.1.2

Call Center

POD: COL-CC

- **When to use**: if you require a call center, help desk, or technical support solution with call queuing and reporting capabilities
- **Prerequisites**: COL-VOICE
- **Required**: OPS-NTP
- **Has Sub-PODs**: Go to 2.1.3

Conferencing

POD: COL-CONF

- **When to use**: if you require advanced conferencing services for voice (audio), video, and/or web sharing capabilities
- **Prerequisites**: COL-VOICE
- **Required**: --
- **Has Sub-PODs**: Go to 2.1.4

Presence

POD: COL-PRS

- **When to use**: if you require IM capabilities and learning about a user’s availability within the voice solution
- **Prerequisites**: COL-VOICE
- **Required**: --
- **Has Sub-PODs**: Go to 2.1.5

Video

POD: COL-VIDEO

- **When to use**: if you require using one (or more) dedicated video endpoints in conference rooms, boardrooms, auditoriums, and other shared environments
- **Prerequisites**: COL-VOICE
- **Required**: QOS
- **Has Sub-PODs**: Go to 2.1.6

2.1.1 Voice

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for the voice solution:

On-Premise	**Cisco - Unified CM** If you require between 1,000 to 10,000+ phone endpoints using an enterprise on-site solution	**Cisco – Unified BE** If you require up to 5,000 phone endpoints using an enterprise on-site solution. Includes support for Messaging
	Avaya - Aura If you require between 1,000 to 36,000+ phone endpoints using an enterprise on-site solution	

Integrated	**Cisco – ISR with CME** If you require up to 450 phone endpoints using an enterprise on-site solution integrated into a Cisco ISR series router	**Fortinet – FortiVoice** If you require up to 2,000 phone endpoints using an enterprise on-site solution. Includes support for Messaging and Call Center
	FreePBX If you require up to 1,000 phone endpoints using an open-source on-site solution. Includes support for Messaging, Call Center, and Presence	**Allworx – Connect** If you require up to 180 phone endpoints using an enterprise on-site solution. Includes support for Messaging and Call Center

Integrated / Cloud	**3CX** If you require a cloud-based PSTN solution using either an on-site or cloud-based phone system. This solution is based on the number of concurrent calls which can support between 4 and 1024 concurrent calls. Includes support for Messaging and Call Center.	**Shoretel – Connect Onsite / Cloud** If you require up to 100 phone endpoints using an SMB on-site (or cloud-based) solution. Includes support for Messaging and Call Center.

Deployment

Select one (or more) of the following PODs that will be used in the voice solution:

	Voice Topology	**Phone System**	**Voice Gateway**
	Endpoint – IP Phone	**Extension Schema**	**Features**
	Dial Plan		

Voice Topology

POD: COL-VOICE-TOP

- **When to use**: this is required to determine how the voice solution will be deployed based on the phone system that is used in the environment
- **Prerequisites**: COL-VOICE
- **Required**: --
- **Has Sub-PODs**: Go to 2.1.1.1

Phone System

POD: COL-VOICE-SYSTEM

- **When to use**: this is a required component in the voice solution and the system type will vary based on the number of phones endpoints
- **Prerequisites**: COL-VOICE-TOP
- **Required**: --
- **Has Sub-PODs**: Go to 2.1.1.2

Voice Gateway

POD: COL-VOICE-VGW

- **When to use**: if you require inbound and outbound external calling in the voice environment
- **Prerequisites**: COL-VOICE-TOP, COL-VOICE-SYSTEM
- **Required**: COL-VOICE-DP
- **Has Sub-PODs**: Go to 2.1.1.3

Endpoint - IP Phone

POD: COL-VOICE-PHONE

- **When to use**: determine what type of phone endpoints will be used in the environment
- **Prerequisites**: COL-VOICE-SYSTEM
- **Required**: SW, PWR-POE, OPS-DHCP
- **Has Sub-PODs**: Go to 2.1.1.4

Extension Schema

POD: COL-VOICE-EXT

- **When to use**: this is required to determine the format of the extensions used in the environment
- **Prerequisites**: COL-VOICE-SYSTEM
- **Required**: --
- **Has Sub-PODs**: Go to 2.1.1.5

Dial Plan

POD: COL-VOICE-DP

- **When to use**: it is required to determine what type of calling rules should be setup on the phone system
- **Prerequisites**: COL-VOICE-SYSTEM
- **Required**: --
- **Has Sub-PODs**: Go to 2.2.1.6

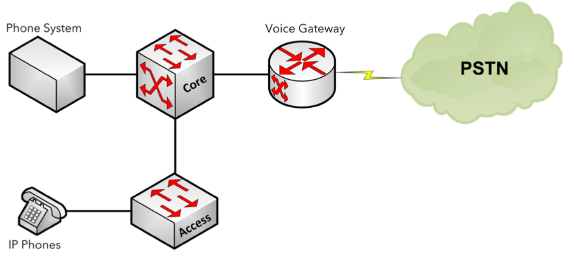
2.1.1.1 Voice Topology

Select one of the following voice topologies that will be used:

	Single Site	**Centralized Multi-Site**	**Partial Centralized Multi-Site**
	Distributed Multi-Site	**Cloud based Solution**	

Single Site

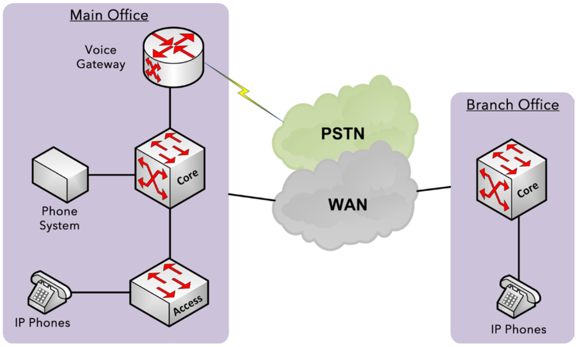
POD: COL-VOICE-TOP-S



- **When to use**: if you require using voice services at a single location
- **Prerequisites**: COL-VOICE-TOP
- **Required**: COL-VOICE-SYSTEM, COL-VOICE-VGW, COL-VOICE-PHONE
- **Has Sub-PODs**: --
- **Components**: Phone System, Voice Gateway/PSTN, Phone Endpoints
- **Description**: in this POD, a phone system is deployed at a single location likely connected into the Core or within the server farm with other voice related servers. The voice gateway, used for external calling, would be connected into the Core switch. And the phone endpoints would be connected into the access switches.

Centralized Multi-Site

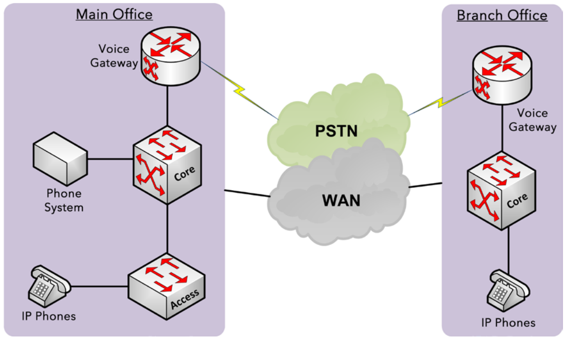
POD: COL-VOICE-TOP-MS1



- **When to use**: if you require using voice services across multiple sites using a phone system and voice gateway located at the main office
- **Prerequisites**: WAN, COL-VOICE-TOP
- **Required**: COL-VOICE-SYSTEM, COL-VOICE-VGW, COL-VOICE-PHONE
- **Has Sub-PODs**: --
- **Components**: Phone System, Voice Gateway/PSTN, Phone Endpoints
- **Description**: in this POD, a centralized phone system and voice gateway are deployed at the main office. They will likely be connected to the Core switch. The phone endpoints would be connected to the access switches. At the remote sites, they would only have phone endpoints attached to their access switches. All phones would register with the phone system and all external calling would occur from the voice gateway at the main office.

Partial Centralized Multi-Site

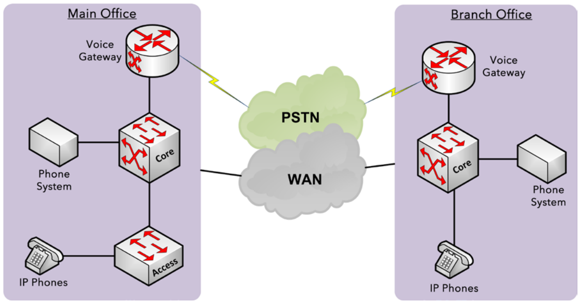
POD: COL-VOICE-TOP-MS2



- **When to use**: if you require using voice services across multiple sites using a centralized phone system at the main office. And require each site to do external calling locally and not over the WAN through another site.
- **Prerequisites**: WAN, COL-VOICE-TOP
- **Required**: COL-VOICE-SYSTEM, COL-VOICE-VGW, COL-VOICE-PHONE
- **Has Sub-PODs**: --
- **Components**: Phone System, Voice Gateway/PSTN, Phone Endpoints
- **Description**: in this POD, a centralized phone system is deployed at the main office. They will likely be connected to the Core switch. The phone endpoints would be connected to the access switches. At the remote sites, they would have phone endpoints attached to their access switches. All phones would register with the phone system. Each site would have their own voice gateway router used for external calling at that local site.

Distributed Multi-Site

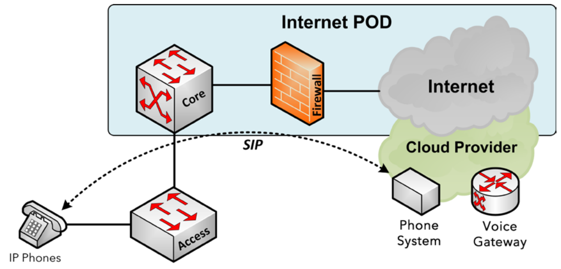
POD: COL-VOICE-TOP-MS3



- **When to use**: if you require using voice services across multiple sites without a WAN and don't want to route voice traffic over VPN tunnels. Or if voice services will be managed differently at each site.
- **Prerequisites**: WAN, COL-VOICE-TOP
- **Required**: COL-VOICE-SYSTEM, COL-VOICE-VGW, COL-VOICE-PHONE
- **Has Sub-PODs**: --
- **Components**: Phone System, Voice Gateway/PSTN, Phone Endpoints
- **Description**: in this POD, a standalone phone system and voice gateway would be deployed at each site on the network. They will likely be connected into their local Core switch. All phone endpoints would be connected to the access switches and will register with their local phone system. Each site would have their own voice gateway used for external calling at that local site. For inter-site calling, SIP trunks would be established between the phone systems where needed.

Cloud based Solution

POD: COL-VOICE-TOP-CLD



- **When to use**: if you require all voice services (phone system, voice gateway, PSTN) to be managed by a cloud voice provider. The phone endpoints would connect to the cloud phone provider to access all voice features and external calling.
- **Prerequisites**: INET, COL-VOICE-TOP
- **Required**: COL-VOICE-SYSTEM, COL-VOICE-PHONE
- **Has Sub-PODs**: --
- **Components**: Phone System + PSTN (Cloud), Phone Endpoints
- **Description**: in this POD, the phone system and voice gateway are deployed (managed) at a cloud provider. The site would only have phone endpoints connected to the access switches and will register with the cloud-based phone system for calling and access to the supported voice features.

Configuration

Below are required, recommended, and optional configuration when deploying the voice topology on the network:

Required	• **Quality of Service (QoS):** should be implemented on all edge ports (on the Access switch) and all uplink/downlink ports including the Router WAN ports. It is recommended to use AutoQoS if you are using Cisco Catalyst switches.

Recommended	• **Multicast**: should be enabled in the environment to work with Music on Hold (MoH) services especially if it will be used over a WAN to remote sites with voice endpoints.

Optional	• None Available

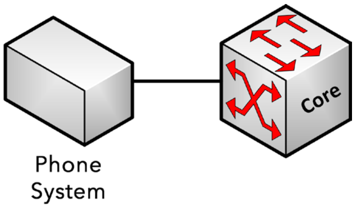
2.1.1.2 Phone System

Select one of the following phone system deployments that will be used:

	On-Premise Deployment	**On-Premise (Cluster) Deployment**	**Integrated Deployment**
	Cloud Deployment		

On-Premise Deployment

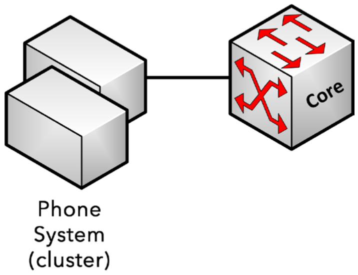
POD: COL-VOICE-SYSTEM-OP1



- **When to use**: if you require an on-site phone system to support up to 500 and 1,000+ users without high availability
- **Prerequisites**: Voice Topology (COL-VOICE-TOP-S or COL-VOICE-TOP-MS*), Vendor (On-Premise)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Phone System
- **Description**: in this POD, a single phone system (physical or virtual) is deployed without any redundancy requirements.

On-Premise (Cluster) Deployment

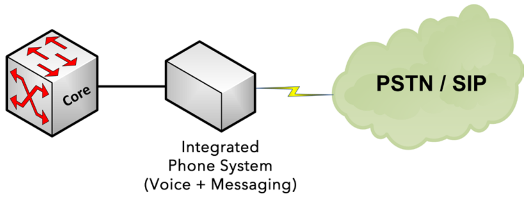
POD: COL-VOICE-SYSTEM-OP2



- **When to use**: if you require an on-site phone system to support over 1,000 users and/or require high availability
- **Prerequisites**: Voice Topology (COL-VOICE-TOP-S or COL-VOICE-TOP-MS*), Vendor (On-Premise)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Phone System(s)
- **Description**: in this POD, one (or more) phone systems (physical or virtual) is deployed to support redundancy. Or to support a higher number of phone endpoints.

Integrated Deployment

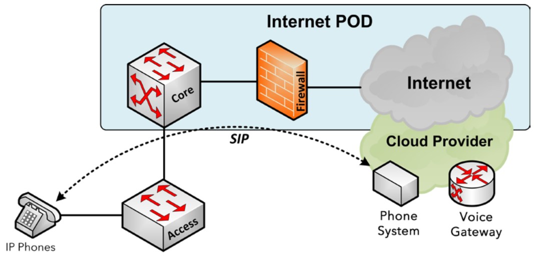
POD: COL-VOICE-SYSTEM-INTG



- **When to use**: if you require an on-site single phone system integrated with the voice gateway to support up to 1,000 phone endpoints
- **Prerequisites**: Voice Topology (COL-VOICE-TOP-S or COL-VOICE-TOP-MS1 or MS3), Vendor (Integrated)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Integrated Phone System
- **Description**: in this POD, a single phone system (integrated with the voice gateway) is used for all voice services as shown in the picture above. This includes support for SIP trunks, Analog lines, and/or PRI circuits for external calling based on the phone system.

Cloud Deployment

POD: COL-VOICE-SYSTEM-CLD



- **When to use**: if you require using a cloud-based phone system and PSTN deployment
- **Prerequisites**: Voice Topology (COL-VOICE-TOP-CLD), Vendor (Cloud)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Phone System (Cloud)
- **Description**: in this POD, the phone system and voice gateway are deployed (managed) at a cloud provider. The site would only have phone endpoints connected to the access switches and will register with the cloud-based phone system for calling and access to the voice features.

Configuration - General

Below are required, recommended, and optional configuration when deploying a general phone system on the network:

Optional	• **Base Phone Features**: these are basic phone features supported on all phone endpoints without any required configuration. They include Placing/Receiving Calls, Call Forwarding, Transfer, Call Park, Speed Dial, and Redial. • **Conferencing**: a phone feature that provides the ability to share a single call with multiple participants. The user can build a conference call directly from their phone then add multiple callers to the active conference that is setup. This is called an Ad-Hoc conferencing setup. • **Paging**: a phone feature that allows callers to send one-way broadcast messages across the voice network. Implementing the paging feature will vary based on the phone system that is used. You can use a third-party paging system such as Bogen TAMB which connects into a stereo amp and to an FXO port on the voice gateway router. Or there could be paging capabilities built-in with the phone system which will use the IP phones as the speaker system. • **Intercom**: a phone feature that allows callers to setup a two-way channel between two phones. Implementing the intercom feature will vary based on the phone system that is used. • **Fax**: if you require users to send and receive digital documents through the voice network. Implementing fax services will vary based on the phone system that is used. You can use a standalone analog fax machine which would be plugged into an FXS port for sending and receiving fax messages. You can use a dedicated third-party fax machine server such as a Castelle Fax Server. Or fax messages can be sent and received over IP (Fax over IP). The fax messages would be converted to a TIFF format then emailed to the intended fax user. This will typically be T.37 or T.38 faxing depending on what is supported in the voice environment.

Configuration – Cisco Unified CM, Unified CM BE

Below are required, recommended, and optional configuration when deploying a Cisco Unified CM (or Unified CM Business Edition) phone system on the network:

Required	• **Partitions & Calling Search Spaces (CSS):** to provide a level of security where voice endpoints (e.g. IP Phones) can only place calls with devices (or directory numbers) within their group called a Calling Search Space (CSS). Each directory number (e.g. extension) or route pattern would be associated to a partition. These partitions are assigned to a CSS group. • **Regions**: determine the codec used for calls within a location or between other locations across the WAN. By default, phones will use G.711 codec for intra/inter-site calling. • **Outbound Calling**: determine the dial plan and its associated route patterns that will be used for external calling out to the PSTN. • **Inbound Calling**: determine the number of digits you want the PSTN provider to pass down. Most PSTN providers will send the last four digits of the DID number to the client's voice gateway. For example, if someone is calling DID 925-230-2203 then the PSTN provider will only forward "2203" to the voice gateway.

Recommended (1/2)	• **Change Hostname to IP Address**: its recommended to change the Cisco Unified CM Publisher/Subscriber/TFTP server host name to its IP address, which removes the dependency of DNS for the phones. • **Partitions**: it is recommended to add the following type of partitions on the system to include Phones/Internal, Emergency Calling, Local Calling, Long Distance Calling, International Calling, Toll Free Calling, and 411/611 Calling. • **Calling Search Spaces based on Medal Class**: create CSS groups based on a medal class of Gold, Silver, and Bronze. A "Gold CSS" will allow calls anywhere. "Silver CSS" will allow only Local, 911, LD, and Internal calling. This is ideal for most phones and employees. And a "Bronze CSS" will allow only Local, 911, and Internal calling. This is ideal for phones in the lobby and public areas. • **Calling Search Spaces based on Calling Hierarchy**: create CSS groups based on a calling hierarchy structure. For example, a "CSS_Base" group can be applied to all phones globally to allow 911 and internal calling. Then one of the following CSS groups can be applied directly to a directory number. (1) "CSS_LocalPSTN" allows only local calling. (2) "CSS_NationalPSTN" allows Local and LD calling. And (3) "CSS_InternationalPSTN" allows Local, LD, and International calling. • **Regions for Intra-Site Calling**: for calls within a site, the region should be configured for the G.722 or G.711 codec (80 kbps per call). There are no limits to the number of calls allowed within a site. • **Regions for Inter-Site Calling**: for calls between sites over the WAN, the region should be configured for the G.729 codec (24 kbps per call). For sites with 500 users, the default setting is two inter-site calls (48 kbps). For sites with 10,000 users, the default is eight inter-site calls (192 kbps).

Recommended (2/2)

- **LDAP Integration**: for end-user authentication integrate the Directory Services (e.g. Active Directory, Open Directory) environment using LDAP with the phone system (Cisco Unified CM and Unified CM BE). This will allow users to access the “User Options” page using their AD credentials to make changes to their IP Phone and directory number. This is a best practice for maintaining a single centralized location for all user authentication on the network.
- **Real-Time Monitoring Tool (RTMT):** an application on Cisco Unified CM which connects to the phone system to provide system resource reports (CPU, Memory), logs, and active call activity.
- **Music-On Hold over WAN**: MoH at the main office should be streamed using multicast from the phone system. MoH at the branch offices should be streamed directly from its local voice gateway and not across the WAN consuming network resources.

Optional (1/2)

- **AAR**: if you require voice calls between sites over the WAN to be automatically re-routed across the PSTN if there are several active calls being established at one time.
- **Medianet**: using Medianet technologies within the network will help to simply and improve the quality of the voice deployment.
- **Call Detailed Records (CDR):** provide reports of calls placed and received by phones in the voice environment.
- **Transcoding**: provides the ability to translate one codec (like G.729) to another codec (like G.711). If you are using a software conferencing solution among the remote sites, transcoding can be enabled on the WAN Aggregation router (or Voice Gateway) where a conference call from a remote site to the main office would use G.729. At the main office, the router would transcode that stream to use G.711 since the software conferencing solution only supports G.711.
- **Device Mobility**: an enhanced feature that allows a user's IP phone to roam between sites. This feature works when the Cisco Unified CM phone system uses the IP Phone's IP subnet to determine the physical location of the phone.

Optional (2/2)	• **Call Pickup**: a phone feature that provides the ability to pick-up a ringing call from another phone within the same group. • **Extension Mobility**: a phone feature that can dynamically configure a phone according to an authenticated user's device profile. When a user login to an IP phone with their username and PIN, their device profile will be uploaded to that IP phone. • **Single Number Reach (Mobile Connect):** a phone feature that provides the ability that a ringing extension will ring other phone devices such as mobile phones. • **Conferencing**: a phone feature that provides the ability to share a single call with multiple participants. Conferencing can either be hardware based (from the voice gateway) or software based (from the phone system). Conferencing can be setup where the user can build a conference bridge directly from their phone and have callers dial directly into the conference call. This feature is called MeetMe on Cisco Unified CM. Or the user can build a conference call directly from their phone then add multiple callers to the active conference that is setup. This is called an Ad-Hoc conferencing setup

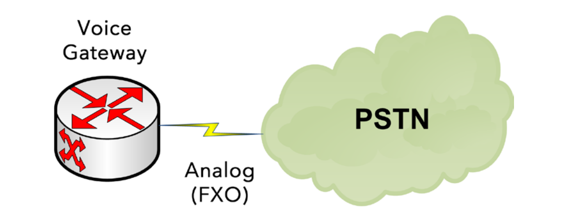
2.1.1.3 Voice Gateway

Select one (or more) of the following voice gateway deployments that will be used:

🟩	**Voice Gateway with Analog**	**Voice Gateway with PRI**	**Voice Gateway with SIP Trunk**

Voice Gateway with Analog

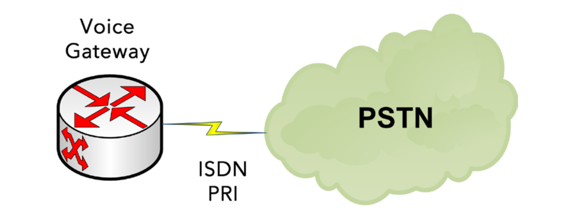
POD: COL-VOICE-VGW-ANALOG



- **When to use**: if you require up to 4 concurrent calls (placed or received) in the voice environment. This is common for small sized networks.
- **Prerequisites**: COL-VOICE-VGW
- **Required**: Router (FXO)
- **Has Sub-PODs**: --
- **Components**: Voice Gateway
- **Description**: in this POD, the voice gateway would be connected to the PSTN using one (or more) analog lines. Each analog line can support 1 concurrent call (placed or received). As a best practice, it is recommended to use no more than 4 analog connections (using FXO module) on the voice gateway router.

Voice Gateway with PRI

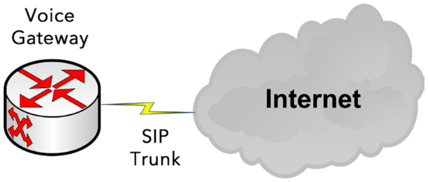
POD: COL-VOICE-VGW-PRI



- **When to use**: if you require up to 23 (or higher) concurrent calls (placed or received) in the voice environment. This is common for SMB, medium, to large sized networks.
- **Prerequisites**: COL-VOICE-VGW
- **Required**: Router (PRI)
- **Has Sub-PODs**: --
- **Components**: Voice Gateway
- **Description**: in this POD, the voice gateway would be connected to the PSTN using one (or more) ISDN PRI circuits. Each PRI circuit can support up to 23 concurrent call (placed or received) as shown in the picture above.

Voice Gateway with SIP Trunk

POD: COL-VOICE-VGW-SIP



- **When to use**: if you require up to 23 (or higher) concurrent calls (placed or received) in the voice environment without using a digital circuit (e.g. Analog, PRI). This is a very popular choice for external calling along with minimal costs compared to the other options.
- **Prerequisites**: INET, COL-VOICE-VGW
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Voice Gateway
- **Description**: in this POD, the voice gateway would build a SIP trunk to a SIP phone provider over the Internet as shown in the picture above. Based on the SIP service plan purchased, it can support up to 23 concurrent calls (placed or received).

Configuration – Cisco Unified CM, Unified CM BE

Below are required, recommended, and optional configuration when deploying a voice gateway on the network with Cisco Unified CM (or Unified CM BE) as the phone system:

Required	• **DSP Resources**: if you are using a Cisco Voice Router, they are required to have packet voice digital signal processor (DSP) modules installed to perform any voice, transcoding, and conferencing services. The number of DSP and PVDMs needed is based on the total number of voice sessions expected. These voice sessions can be (1) voice calls, (2) transcoding, and (3) conferencing. For example, a "PVDM3-64" can support up to 64 voice sessions. This means, that PVDM can accommodate up to one voice T1 (24 voice sessions) and five 8-party conference sessions (40 voice sessions).

Recommended	• **SRST**: this is recommended for all branch offices using a WAN to communicate back to the phone system cluster. If the phone system fails (with no secondary phone system available) or if the WAN connection fails for a remote site, the IP Phones can use SRST fallback. In SRST fallback mode, the phones will register with the local voice gateway to place and receive calls until the phone system is available again. • **Redundant PRI Circuits**: it’s recommended to use a second PRI or analog lines if the primary PSTN circuit should fail. Using different PSTN providers can provide higher reliability, but there may be challenges for using the same DID block between two different PSTN providers. This redundancy option is common for most business size networks with moderate voice calling requirements. Redundant PRIs can also be helpful if there is a high call volume in the environment.

Optional	• None Available

2.1.1.4 Endpoints – IP Phones

Select one (or more) of the following type of phone endpoints that will be used:

Employees	**Executives**	**Receptionist / Help Desk**
Conference Room	**Lobby / Break Room / Kitchen**	**Mobility**
Video Endpoint		

Employees

POD: COL-VOICE-PHONE-EMP

- **When to use**: determine the number of phone endpoints that will be used by regular employees in the voice environment
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Phone endpoint
- **Description**: this endpoint will typically be a standard phone with 1-2 line appearances with a gray-scale display as shown in the picture above (e.g. Cisco 7821).

Executives

POD: COL-VOICE-PHONE-EXC

- **When to use**: determine the number of phone endpoints that will be used by executives (or management) in the voice environment
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Phone endpoint
- **Description**: this endpoint will typically be a standard phone with 2-3+ line appearances with a color display and other advanced capabilities as shown in the picture above (e.g. Cisco 8841).

Receptionist / Help Desk

POD: COL-VOICE-PHONE-REP

- **When to use**: determine the number of phone endpoints that will be used by receptionist and/or help desk employees in the voice environment
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Phone endpoint
- **Description**: this endpoint will typically be a standard phone with multiple line appearances to support many incoming/outgoing calls as shown in the picture above (e.g. Cisco 7861).

Conference Room

POD: COL-VOICE-PHONE-CONF

- **When to use**: determine the number of phone endpoints that will be used in conference rooms in the voice environment
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Phone endpoint
- **Description**: this endpoint will typically be a conference room based phone with an advanced speaker-phone configuration as shown in the picture above (e.g. Cisco 7937G).

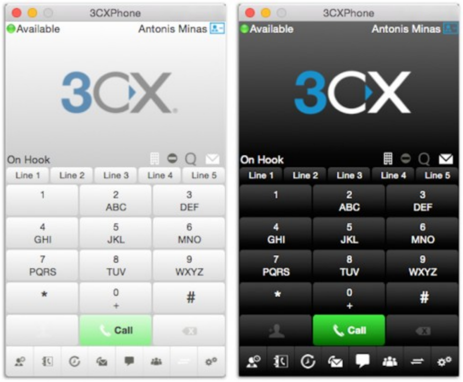
Lobby / Break Room / Kitchen

POD: COL-VOICE-PHONE-LBK

- **When to use**: determine the number of phone endpoints that will be used in the lobby area, break room, locker room to kitchens in the voice environment
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Phone endpoint
- **Description**: this endpoint will typically be a basic phone with 1 line appearance with no display as shown in the picture above (e.g. Cisco 6901).

Mobility

POD: COL-VOICE-PHONE-MOB



- **When to use**: determine the number of phone endpoints that will be used by employees, executives, to contractors in the voice environment that do not require a physical phone
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Phone endpoint
- **Description**: this endpoint is a software-based phone endpoint, as shown in the picture above, that can be installed on person's computer (or mobile device). This phone choice is becoming very popular in the voice environment today.

Video Endpoint

POD: COL-VOICE-PHONE-VID

- **When to use**: if you require some of the physical phone endpoints to have video telephony capabilities
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Video Phone endpoints
- **Description**: in this POD, some users with phone endpoints will have IP phones with video capabilities or a video desktop unit on their desk.

Configuration

Below are required, recommended, and optional configuration when adding phones on the network:

Required

- **DHCP**: required for the IP Phones to know how to connect to the phone system (e.g. Cisco Unified CM). DHCP can be configured either on the network or on a DHCP server (recommended). Add "Option 150" pointing to the IP address of the TFTP server (in most cases the phone system like Cisco Unified CM) which is responsible for the phones to download their configuration and the latest firmware.
- **Phone Firmware**: if you are using a Cisco Phone System, the default firmware on the phone endpoints will be SCCP. Otherwise, the phone endpoint would use the SIP phone firmware. **Note**: Cisco phones can also support SIP firmware if needed.

Recommended

- **Voice VLAN**: as a best practice configure a Voice VLAN for all voice traffic (e.g. IP Phones, Voice Gateway) separate from the production data network configured in one (or more) Data VLANs. Cisco Discovery Protocol (CDP) is required to provide the Cisco IP phones configuration details such as the Voice VLAN it should use, power requirements, and the ability to prioritize traffic. As a result, 802.1Q Trunking is used between all switches and the IP Phone to provide Data and Voice VLAN assignment.
- **Phone with Switch Port**: if you are using a physical phone endpoint, it is recommended to get a phone with an integrated switch port. This way, the user's PC would be connected to the phone and the phone would be directly connected to the access switch enabled for PoE.
- **Power over Ethernet (PoE):** it is recommended to provide power to the IP Phones from its connected access switch. This can avoid using a phone adapter for all phones which can cluster a user's work space.
- **Phone Firmware using SIP**: if you require the phone endpoints to use SIP firmware for connecting with the phone system and supporting capabilities such as URI dialing. Including the ability to use affordable soft-phones instead of a physical phone.

Optional

- **Phone Components**: determine the type of phone endpoints needed based on the number of line appearances (for extensions and speed dials), display (e.g. Color, Gray-scale, Touchscreen), speaker-phone support, to having an integrated switch port.

2.1.1.5 Extension Schema

Select one of the following extension schemas that will be used in the solution:

3-Digit Extension	**4-Digit Extension**	**6-Digit Extension**
7-Digit Extension		

3-Digit Extension

POD: COL-VOICE-EXT-3D

- **When to use**: ideal for small and SMB sized environments with up to 10 and 500 voice endpoints
- **Description**: for this schema, extension 301 could be a user's extension at a single location.

4-Digit Extension

POD: COL-VOICE-EXT-4D

- **When to use**: ideal for SMB and medium sized environments with up to 300 and 999 voice endpoints
- **Description**: for this schema, extension 5100 could be a user's extension at a single location. A site ID could also be used with this schema where the "5" could be the site-ID for the extension.

6-Digit Extension

POD: COL-VOICE-EXT-6D

- **When to use**: ideal for Medium to Large sized environments with 90 sites or less with thousands of voice endpoints
- **Description**: for this schema, the extension format would be something like "SS + XXXX". Where "SS" would be a two-digit site code to accommodate up to 90 sites (10-99 sites). And "XXXX" would be four-digits for the actual extension at the site. For example, using extension 106778, means that the site code would be 10 and the extension at the site would be 6778.

7-Digit Extension

POD: COL-VOICE-EXT-7D

- **When to use**: ideal for Large sized environments with more than 90 sites with thousands of voice endpoints
- **Description**: for this schema, the extension format would be something like "SSS + XXXX". Where "SSS" would be a three-digit site code to accommodate up to 900 sites (100 to 999 sites). And "XXXX" would be four-digits for the extension at the site. For example, using extension 1016778, means that the site code would be 101 and the extension at the site would be 6778.

2.1.1.6 Dial Plan

Select one (or more) of the following dial plans that will be used in the solution:

🟩	**NANP Dial Plan**		

NANP Dial Plan
POD: COL-VOICE-DP-NANP
Emergency Dialing: 911, 9.911 **Local Dialing**: 9.[2-9]XXXXXX **National (Long Distance) Dialing**: 9.1[2-9]XX[2-9]XXXXXX **International Dialing**: 9.011!, 9.011# **Toll Free Dialing**: 9.1888[2-9]XX XXXX, 9.1877[2-9]XX XXXX, 9.1866[2-9]XX XXXX
• **When to use**: recommended dial plan for phone systems located in North America (e.g. US) • **Description**: this dial plan consists of route patterns (shown above) used for outbound calling through the PSTN based on the recommended dial plan and country. These route patterns would be assigned to their appropriate route partition. These patterns all include an access code of “9” which is recommended when placing outbound calls from the voice environment.

2.1.2 Messaging

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for the messaging solution:

On-Premise	**Cisco – Unity Connection** If you require a standalone enterprise on-site solution to support 3,000 voice mailboxes.	

Integrated / Cloud	**Cisco – ISR with CUE** If you require voice mailboxes up to 500 users using a small business on-site solution integrated into a Cisco ISR series router.	**Fortinet – FortiVoice** If you require up to 2,000 phone endpoints using an enterprise on-site solution with voicemail support. Includes support for Voice and Call Center
	FreePBX If you require up to 1,000 phone endpoints using an open-source on-site solution with voicemail support. Includes support for Voice, Call Center, and Presence	**Allworx – Connect** If you require up to 180 phone endpoints using an enterprise on-site solution with voicemail support. Includes support for Voice and Call Center
	3CX If you require a cloud-based PSTN solution using either an on-site or cloud-based phone system with voicemail support.	**Shoretel – Connect Onsite / Cloud** If you require up to 100 phone endpoints using an SMB on-site (or cloud-based) solution with voicemail support.

Combined	**Cisco – Unified BE** If you require up to 5,000 phone endpoints using an enterprise on-site solution with support up to 1,000 voice mailboxes. Includes support for Voice.	

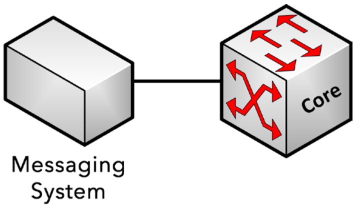
Deployment

Select one of the following messaging deployments that will be used in the solution:

	On-Premise Deployment	**On-Premise (Cluster) Deployment**
	Combined Deployment	

On-Premise Deployment

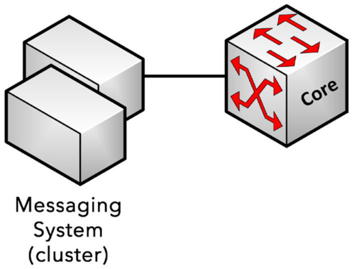
POD: COL-MSG-SINGLE



- **When to use**: if you don't require high-availability for the messaging system
- **Prerequisites**: COL-MSG, Vendor (On-Premise)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Messaging server
- **Description**: in this POD, a single messaging system is located within the server farm with the other voice related servers.

On-Premise (Cluster) Deployment

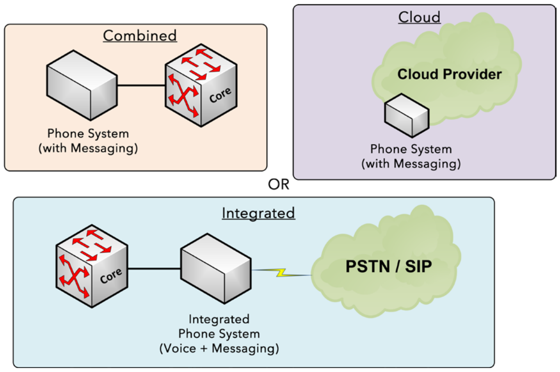
POD: COL-MSG-CLUSTER



- **When to use**: if you require high-availability for the messaging system to provide minimal downtime if there is a failure
- **Prerequisites**: COL-MSG, Vendor (On-Premise, CUC)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Messaging servers
- **Description**: in this POD, multiple messaging servers are clustered together using a publisher server and multiple subscriber servers. This cluster is located within the server farm with the other voice related servers.

Combined Deployment

POD: COL-MSG-COMB



- **When to use**: if the current phone system deployed supports messaging services
- **Prerequisites**: COL-MSG, Vendor (Integrated, Cloud, Combined)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Phone system
- **Description**: in this POD, the existing phone system deployed in the environment supports messaging services.

Configuration – Cisco Unity Connection

Below are required, recommended, and optional configuration when deploying a Cisco Unity Connection messaging solution on the network:

Required

- **Voicemail Accounts**: determine the number of voice mailboxes that will be used.
- **Pilot Numbers**: pilot numbers are required for all voicemail/messaging services that will be used such as access to the voicemail system, auto-attendant (AA) menu, and access to the greeting administration menu to record the greetings for the AA menu.
- **Voice Ports**: determine the number of ports used between the voicemail server and the phone system. The ports relate to the total concurrent number of calls (1) sent to a subscriber's voice mailbox. (2) Users checking their voicemail messages. (3) Message Waiting Indicator (MWI) notifications. And (4) callers routed to an Auto-Attendant (AA) menu. For the total number of voice ports, it is recommended to dedicate 25% of the voice ports for MWI and the other 75% for voicemail and AA purposes.

Recommended

- **Backups**: always do scheduled backups on the VM/UM server. This way you can rebuild the server in a couple of hours if the messaging system encounters a failure. Cisco Unity Connection provides scheduled backups through the Disaster Recovery System, which is highly recommended.
- **Strong Passwords**: it is recommended to use complex PIN/passwords for the voicemail accounts for increased security
- **Password Reset Policy**: voicemail account PIN/Passwords should be reset every 180 days
- **Account Lockout**: account lockouts should be enabled if three failed login attempts occur

Optional

- **Auto-Attendant (AA):** if you require providing an automated menu for callers to access a directory listing and other information/resources available.
- **Voice Recognition**: if you require providing the capability for users to use voice commands to access various voice features and placing calls.
- **Email Notifications**: if you require voicemail messages to be sent via email as an attachment or receive a notification email that a new message has arrived.
- **Unified Messaging**: provide TTS (Text-to-Speech) capabilities for users to have their actual email messages read back to them through any phone endpoint. Unified messaging also provides synchronization of voicemail messages with a user's email inbox. If a user hears a new message through their email client (e.g. Outlook), it will automatically sync that status back to the VM/UM server turning off the notification (MWI) on the user's phone.

2.1.3 Call Center

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for the call center solution:

On-Premise	**Cisco – Unified CCE** If you require a standalone commercial on-site solution to support 500+ call center agents	**Cisco – Unified CCX** If you require a standalone commercial on-site solution to support up to 400 call center agents

Integrated / Cloud	**Shoretel – Connect Onsite / Cloud** If you require up to 100 phone endpoints using an SMB on-site (or cloud-based) solution with call center support.	**Fortinet – FortiVoice** If you require up to 2,000 phone endpoints using an enterprise on-site solution with basic call center support. Includes support for Messaging and Call Center
	FreePBX If you require up to 1,000 phone endpoints using an open-source on-site solution with basic call center support. Includes support for Messaging, Call Center, and Presence	**Allworx – Connect** If you require up to 180 phone endpoints using an enterprise on-site solution with basic call center support. The solution can support up to 10 queues with 10-60 concurrent calls in all queues. Includes support for Messaging and Call Center
	3CX – Pro / Enterprise If you require a cloud-based PSTN solution using either an on-site or cloud-based phone system with call center support.	

Combined	**Cisco – Unified BE** If you require up to 5,000 phone endpoints using a commercial on-site solution with support up to 100 call center agents. Includes support for Voice, Messaging, and Presence.	

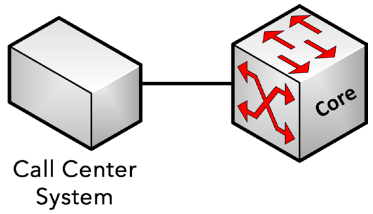
Deployment

Select one of the following call center deployments that will be used in the solution:

On-Premise Deployment	**On-Premise (Cluster) Deployment**
Combined Deployment	

On-Premise System

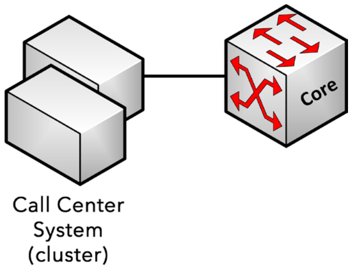
POD: COL-CC-SINGLE



- **When to use**: if you don't require high-availability for the call center system
- **Prerequisites**: COL-CC, Vendor (On-Premise)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Call Center server
- **Description**: in this POD, a single call center system is located within the server farm with the other voice related servers.

On-Premise (Cluster) System

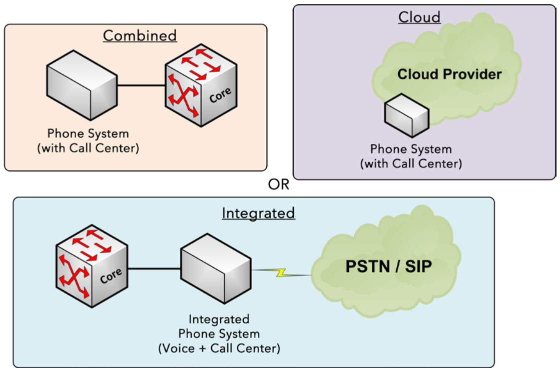
POD: COL-CC-CLUSTER



- **When to use**: if you require high-availability for the call center system to provide minimal downtime if there is a failure
- **Prerequisites**: COL-CC, Vendor (On-Premise, CCX)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Call Center servers
- **Description**: in this POD, multiple call center servers are clustered together using a publisher server and multiple subscriber servers. This cluster is located within the server farm with the other voice related servers.

Combined Deployment

POD: COL-CC-COMB



- **When to use**: if the current phone system deployed supports call center services
- **Prerequisites**: COL-CC, Vendor (Integrated, Cloud, Combined)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Phone system
- **Description**: in this POD, the existing phone system deployed in the environment supports call center services.

Deployment – Cisco Unified CCX

Below are required, recommended, and optional configuration when deploying a call center solution on the network:

Required

- **Calling Queues (CSQ)**: determine the type of queues that will be implemented in the call center. It will likely be a Support queue and/or a Sales queue in the call center environment. Keep in mind that there may be multiple support/sales queues (e.g. IT support, product support, etc.) that may need to be considered.
- **Agent Extension**: each agent should have a dedicated extension that will be part of a call center queue to receive calls.
- **Supervisor & Teams**: for each call queue, determine who will be the supervisor that will be able to monitor the call activity for the queue. Next, determine the agents that will be part of a team covering the same queue that will be supervised.
- **Resources**: each agent with its dedicated extension will be created as a resource. It's important to assign the appropriate skills (e.g. support, sales) to the right agent/resource.
- **Agent Selection**: determine how new calls should be routed to an agent within a specific CSQ. The available options include linear, circular, longest available, most handled contacts, most skilled, and least skilled.
- **MOH/Announcement for Queues**: determine the audio recording for the queues. It can be a music audio file or maybe a company announcement/advertisement.
- **Script for Queues**: determine how the call menu will be programmed when users call into a queue

Recommended

- **Agent Selection using Longest Available**: if you require all new calls to be sent to agents that has been in a "ready state" the longest. This selection ensures that all calls are distributed fairly among all agents in a CSQ (Recommended).
- **Agent Selection using Most Skilled**: if you require your most skilled (tier2, tier3) agents to answer new calls before the least skilled (tier1) agents for providing premium level support.
- **Agent Selection using Least Skilled**: if you require all new calls to be sent to tier1 support agents before they are routed to more skilled agents (tier2 support).
- **Reason Codes**: its recommended to setup Reason codes which reflects the reason why an agent logs out. The recommended reason codes to setup should be: End of Shift, Break, Lunch, Meeting. For example, when an agent needs to logout of a queue, within the agent program a window would pop-up. The pop-up window would present a couple of choices which would be the reason codes. If the user selects "Lunch" then that would be recorded and can be viewed in the generated reports by the supervisor.

Optional

- **Interactive Voice Response (IVR):** determine if Interactive Voice Response (IVR) will be used. IVR involves recorded messages or text-to-speech for responding to caller inputs using DTMF signaling or speech within a CSQ menu tree.
- **Recording/Monitoring**: if you require recording (and/or monitoring) agent sessions on the system. It's important to determine if the vendor solution chosen supports this capability.

2.1.4 Conferencing

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for the conferencing solution:

On-Premise	**Cisco - WebEx** If you require an advanced conferencing solution providing voice, video, and web capabilities (such as doing presentations or anything shown on the presenter's desktop). This solution can be deployed as a standalone enterprise on-site solution or as a cloud-based solution.

Integrated / Cloud	**Shoretel – Connect Onsite / Cloud** If you require up to 100 phone endpoints using an SMB on-site (or cloud-based) solution with advanced conferencing support.	**Fortinet – FortiVoice** If you require up to 2,000 phone endpoints using an enterprise on-site solution with basic voice conferencing. Includes support for Voice, Messaging and Call Center
	FreePBX If you require up to 1,000 phone endpoints using an open-source on-site solution with basic voice conferencing. Includes support for Voice, Messaging, Call Center, and Presence	**Allworx – Connect** If you require up to 180 phone endpoints using an enterprise on-site solution with basic voice conferencing. Includes support for Voice, Messaging and Call Center
	3CX If you require a cloud-based PSTN solution using either an on-site or cloud-based phone system with voice and web conferencing support.	**Cisco – ISR with CME** If you require up to 450 phone endpoints using a commercial on-site solution integrated into a Cisco ISR router with basic voice conferencing. Includes support for Voice

Combined	**Cisco – Unified CM** If you require between 1,000 to 10,000+ phone endpoints using an enterprise on-site solution with basic voice conferencing. Includes support for Voice.	**Cisco – Unified BE** If you require up to 5,000 phone endpoints using a commercial on-site solution with basic voice conferencing. Includes support for Voice, Messaging, and Presence.

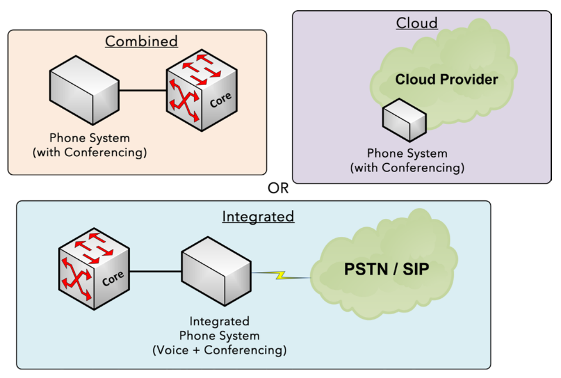
Deployment

Select one of the following conferencing deployments that will be used in the solution:

	Combined Deployment	

Combined Deployment

POD: COL-CONF-COMB



- **When to use**: if the current phone system deployed supports conferencing services
- **Prerequisites**: COL-CONF, Vendor (Integrated, Cloud, Combined)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Phone system
- **Description**: in this POD, the existing phone system deployed in the environment supports conferencing services (voice, video and/or web).

2.1.5 Presence

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for the presence solution:

On-Premise	**Cisco – IM&P** If you require a standalone on-site solution for presence to support between 500 and 5000 users

Integrated / Cloud	**3CX** If you require a cloud-based PSTN solution using either an on-site or cloud-based phone system with presence & chat support	**FreePBX** If you require up to 1,000 phone endpoints using an open-source on-site solution with basic presence support. Includes support for Voice, Messaging, and Call Center

Combined	**Cisco – Unified BE** If you require up to 5,000 phone endpoints using an enterprise on-site solution with presence support for 1000 users. Includes support for Voice and Messaging	

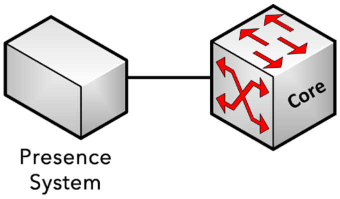
Deployment

Select one of the following presence deployments that will be used in the solution:

	On-Premise Deployment	**On-Premise (Cluster) Deployment**
	Combined Deployment	

On-Premise Deployment

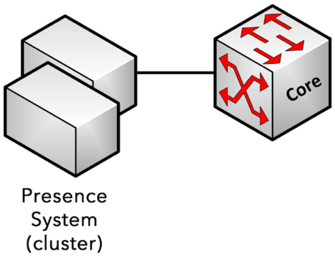
POD: COL-PRS-SINGLE



- **When to use**: if you don't require high-availability for the presence system
- **Prerequisites**: COL-PRS, Vendor (On-Premise)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Presence server
- **Description**: in this POD, a single presence system is located within the server farm with the other voice related servers.

On-Premise (Cluster) Deployment

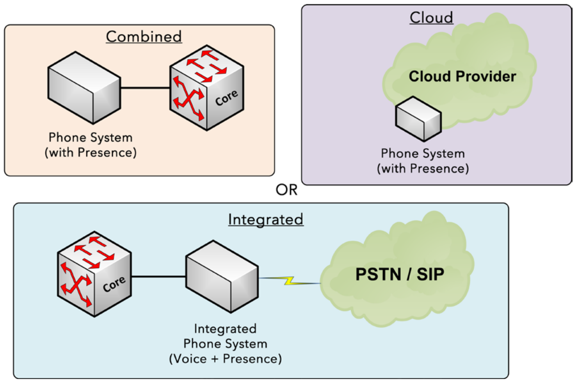
POD: COL-PRS-CLUSTER



- **When to use**: if you require high-availability for the presence system to provide minimal downtime if there is a failure
- **Prerequisites**: COL-PRS, Vendor (On-Premise, IMP)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Presence servers
- **Description**: in this POD, multiple presence servers are clustered together using a publisher server and multiple subscriber servers. This cluster is located within the server farm with the other voice related servers.

Combined Deployment

POD: COL-PRS-COMB



- **When to use**: if the current phone system deployed supports presence services
- **Prerequisites**: COL-PRS, Vendor (Integrated, Cloud, Combined)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Phone system
- **Description**: in this POD, the existing phone system deployed in the environment supports presence services.

2.1.6 Video

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for the video solution:

On-Premise	**Cisco – Telepresence** If you require the video endpoints using the “Rooms and Immersive Systems” to work with the existing Cisco Voice solution already deployed.

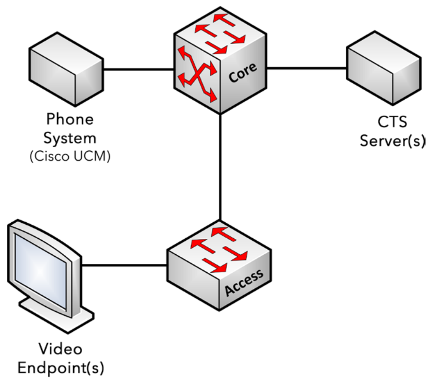
Deployment

Select one (or more) of the following video deployments that will be used in the solution:

	Immersive Video Deployment	**Multipurpose Video Deployment**

Immersive Video Deployment

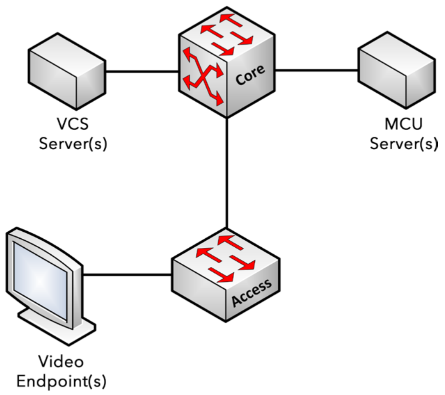
POD: COL-VIDEO-IM



- **When to use**: if you require using a video solution to present a real-life in-person video collaboration experience as if all attendees are in the same room. This is common for large conference rooms.
- **Prerequisites**: COL-VIDEO
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Phone System (UCM), CTS server
- **Description**: in this POD, two server endpoints are required: (1) a Cisco Unified CM system is required to provide call control for the video endpoints. And (2) a Cisco Telepresence Server (CTS) is required for conferencing capabilities with the solution. The communication between the components including the video endpoints involve SIP connections. The two servers would likely be connected to the Core switch as shown in the picture above.

Multipurpose Video Deployment

POD: COL-VIDEO-MP



- **When to use**: if you require using a video solution to allow one (or two) video endpoints to be present in the room for individual high-quality point-to-point conference calls. This is common for meeting rooms, boardrooms, auditoriums, and other shared environments.
- **Prerequisites**: COL-VIDEO
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: VCS server, MCU server
- **Description**: in this POD, two server endpoints are required: (1) Video Communication Server (VCS) is needed to provide call control for the video endpoints. And (2) a Codian Multipoint Control Unit (MCU) is required for conferencing capabilities with the solution. The MCU server component can join multiple video and voice participants in a single conference call. The two servers would likely be connected to the Core switch as shown in the picture above.

Configuration

Below are required, recommended, and optional configuration when deploying a video solution on the network:

Required

- **Quality of Services**: a best practice that should be implemented on the LAN for all ports according to the QoS design (edge ports, uplink/downlink ports, and Router WAN ports if applicable) running video services.
- **Multicast**: should be implemented to provide broadcast video delivery efficiency across the network.

Recommended

- **Video over IP Network**: it is recommended to run your video collaboration traffic over an IP network rather than a public ISDN.
- **Bandwidth Considerations**: It's recommended to allow 23% of the WAN bandwidth for video calls. Each video call will typically consume up to 1.5Mbps. This is a general baseline to start with.
- **Budgetary Considerations**: the price for Telepresence is very expensive. Therefore, if the total travel cost (air travel, hotel, car rental, food, and other related fees) per person exceeds the price of the video endpoint itself then purchasing a Telepresence solution would make business sense.
- **Conference Room Considerations**: for the table in the conference room, it’s recommended to not use dark colors, patterns or glass. Use a natural wood color instead. For the acoustics, do not allow more than 25-30db of sound so it doesn't transmit through the walls.
- **Medianet (Performance Monitor):** used to help simply and improve the quality of the video deployment. It can also help to provide better troubleshooting tools when issues arise on the video network. This includes using media traces for viewing the health of the network components along the path. Medianet services should be enabled on all components within the WAN (HQ & remote site) and LAN PODs.

Optional

- **Media Services**: content recording server where you can record and stream video meetings
- Duo-Video for Sharing Presentations
- **Far End Camera Control (FECC):** allows remote sites to change their viewing angle during a video call
- **Multisite Conferencing**: allow video endpoints with conferencing capabilities to add a third device into a video call
- **Multiway conferencing**: allow video endpoints to start an ad-hoc multi-point call using a standard MCU

2.2 Computing

Select one (or more) of the following Computing PODs that will be used in the design:

	Cloud Computing	**Unified Computing**	

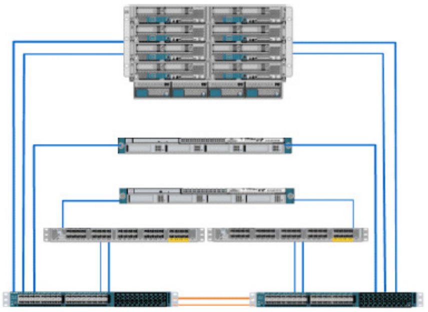
Cloud Computing

POD: COMP-CLD

- **When to use**: if you require (1) providing access to cloud-based applications and services for the endpoints (e.g. Office 365). (2) To provide the capability to manage your server farm in the cloud (e.g. Amazon EC2). Or (3) to build a cloud-based service offering that will be accessed by other customer environments (e.g. IAAS)
- **Prerequisites**: INET, LAN/DC
- **Required**: --
- **Has Sub-PODs**: Go to 2.2.1

Unified Computing

POD: COMP-UC



- **When to use**: if you require building a compute system (traditional and/or HCI) to create a large number of virtual machines based on the amount of storage and compute resources they will have
- **Prerequisites**: DC
- **Required**: --
- **Has Sub-PODs**: Go to 2.2.2

2.2.1 Cloud Computing

Select one (or more) of the following Cloud Computing PODs that will be used in the design:

	IaaS - Framework	**SaaS - Applications**	**PaaS - Platform**

IaaS - Framework
POD: COMP-CLD-IAAS
• **When to use**: if you require hosting servers within the cloud managed by you (or the customer network) • **Prerequisites**: COMP-CLD • **Required**: -- • **Has Sub-PODs**: Go to 2.2.1.1 • **Description**: this POD is an Internet based service (Public cloud) which only has a partial topology type that is deployed. The server farm would be virtualized within a IaaS framework provider (e.g. Amazon AWS). Or it can be used within a Data Center (Private cloud). In a IaaS, the customer is responsible for managing the OS, applications installed, and the data.

SaaS - Applications
POD: COMP-CLD-SAAS
• **When to use**: if you require utilizing cloud-based applications for mail, storage, and other applications instead of managing (or hosting) any servers • **Prerequisites**: COMP-CLD • **Required**: -- • **Has Sub-PODs**: Go to Go to 2.2.1.2 • **Description**: this POD is an Internet based service which is deployed within a hosted provider infrastructure connected to the Internet. There is no topology deployed. In a SaaS, all components (hardware, OS, applications, data) are managed by the cloud provider.

PaaS - Platform
POD: COMP-CLD-PAAS
• **When to use**: if you require utilizing cloud-based platforms • **Prerequisites**: COMP-CLD • **Required**: -- • **Has Sub-PODs**: Go to 2.2.1.3 • **Description**: this POD is an Internet based service which is deployed within a hosted provider infrastructure connected to the Internet. There is no topology deployed. In a PaaS, the customer is responsible for managing the applications installed and the data.

2.2.1.1 IaaS - Framework

Complete each of the design sections below for the solution

Vendor Solutions

Select one of the following vendors that will be used for the IaaS framework:

Vendor Solutions	**Amazon Web Services (AWS)** If you require building a public IaaS using the Amazon Web Services framework	**Microsoft Azure** If you have a Microsoft centric environment and require building a public IaaS using the Microsoft Azure framework to support capabilities like AD synchronization to the cloud
	Google Cloud If you have a Google centric environment and require building a public IaaS using the Google Cloud framework	**OpenStack** If you require building your own private IaaS framework that you can provide to customers for cloud computing services (IaaS, SaaS)

2.2.1.2 SaaS - Applications

Complete each of the design sections below for the solution.

Vendor Solutions

Select one (or more) of the following vendors that will be used for cloud-based applications:

Vendor Solutions	**Mail Applications** If you require using cloud-based mail applications. Some of the most popular products include: Office 365 (Microsoft), Gmail (Google)	**Storage Applications** If you require using cloud-based storage applications. Some of the most popular products include: Dropbox, Box, OneDrive (Microsoft) Google Drive (Google), iCloud Drive (Apple)
	Office Applications If you require using cloud-based document, presentation, and spreadsheet applications. Some of the most popular products include: Office 365 (Microsoft), Google Docs (Google)	**CRM Applications** If you require using cloud-based CRM applications. Some of the most popular vendors/products include: Salesforce, Zoho
	Help Desk Applications If you require using cloud-based help desk applications. Some of the most popular vendors/products include: ServiceDesk Plus (ManageEngine), Manage (ConnectWise), AutoTask	**Voice (Phone System) Applications** If you require using a cloud-based phone system. Some of the cloud-based phone system vendors/products include: Shoretel, 3CX, RingCentral
	Voice (PSTN) Applications If you require using cloud-based PSTN SIP services. Some of the cloud-based SIP providers include: Flowroute, Vonage Business	

2.2.1.3 PaaS - Platform

Complete each of the design sections below for the solution.

Vendor Solutions

Select one (or more) of the following vendors that will be used for cloud-based storage and platforms:

Vendor Solutions	**Amazon AWS - S3** If you require using Amazon AWS's S3 as a storage platform that will be used by other servers / services	

2.2.2 Unified Computing

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for the Unified computing solution:

Traditional	**Cisco – UCS** If you require building a Unified Computing solution for your Data Center using Cisco based hardware without virtualizing the computing, storage, and network resources.	

Hyper Converged (HCI)	**Cisco – HyperFlex** If you require building a HCI solution for your Data Center using Cisco based hardware by virtualizing the computing, storage, and network resources. HyperFlex (HX220, HX240) is based on Cisco UCS hardware using Xeon E5 processors. You must have at least 3 HCI nodes which is scalable up to 8 nodes.	**Nutanix – NX Series** If you require building a HCI solution for your Data Center using Nutanix based hardware by virtualizing the computing, storage, and network resources.
	Riverbed – SteelFusion If you require building a HCI solution for your Data Center using Riverbed based hardware by virtualizing the computing, storage, and network resources.	**VMware – vSAN** If you require building a HCI solution for your Data Center using a VMware based solution.
	Scale Computing – HC3 If you require building a HCI solution for your Data Center using Scale Computing based hardware by virtualizing the computing, storage, and network resources.	

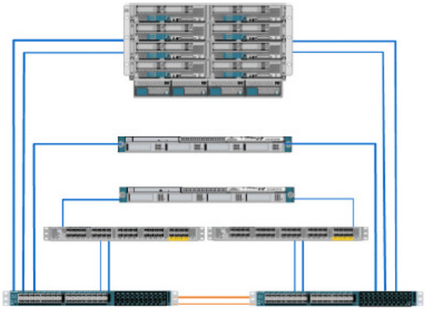
Deployment

Select one (or more) of the following UC deployments that will be used in the solution:

	Traditional Deployment - Unified	**Traditional Deployment - Standalone**	**HCI Deployment**

Traditional Deployment - Unified

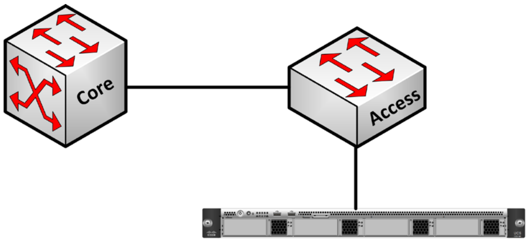
POD: COMP-UC-T-UNF



- **When to use**: if you require using a traditional computing system with one (or more) Cisco UCS B-Series or C-Series servers that can be managed from the Cisco UCS Manager
- **Prerequisites**: Hardware (Traditional - Cisco UCS)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: UCS system, Interconnect switch
- **Description**: in this POD, all of the UCS systems are connected to one (or two) Cisco Interconnect switches where the entire computing solution can be managed from the Cisco UCS Manager (stored on the Interconnect switches). The interconnect switch would connect to the Data Center Core (in a Traditional DC topology) or to one of the Leaf switches (in a SDN topology).

Traditional Deployment - Standalone

POD: COMP-UC-T-STD

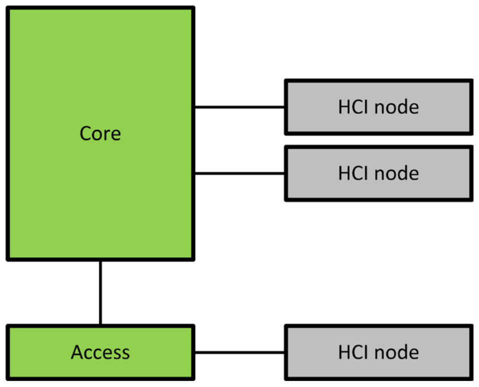


Cisco UCS C-Series Server

- **When to use**: if you require using a traditional standalone computing system (using the Cisco UCS C-Series) that can be managed independently to host several virtual machines
- **Prerequisites**: Hardware (Traditional - Cisco UCS)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: UCS system
- **Description**: in this POD, the UCS system is treated as a standard bare-metal server running a hypervisor to support several virtual machines. Each standalone system would be connected with the other servers on the network. They would be connected to either the DC access switch (in a Traditional 2-Tier DC topology / Cisco Nexus 2200 series) or the Core switch (in a Traditional 1-Tier DC topology / Cisco Nexus 5500 series).

HCI Deployment

POD: COMP-UC-HCI



- **When to use**: if you require consolidating the computing, storage, and network resources to a single platform to lower the number of systems (HCI nodes) used in the data center with centralized management.
- **Prerequisites**: Hardware (Hyper-Converged)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: HCI based systems, Data center switches (core, access)
- **Description**: in this POD, one (or more) HCI nodes are connected into either the Data Center Core or to one of the Access/Leaf switches as shown in the picture above. All of the HCI nodes are managed from a centralized interface like Cisco UCS in a traditional server infrastructure model. Using HCI nodes will require greater performance on the data center switches.

Configuration – Traditional Deployment

Below are required, recommended, and optional configuration when deploying a Cisco Unified Computing solution on the network:

Required

- **Network Adapter**: determine the network adapter that will be used in the selected UCS systems.
- **Physical and Virtual Servers**: determine the number of servers needed for the Data Center based on whether they will use an entire physical blade server or if servers will be virtualized within a single blade server. If there is a mixture of both physical and virtual servers include both numbers.
- **Server Resources**: determine the resources that will be used for each physical and virtual server. This will include resources such as CPU, Memory, LAN & SAN connectivity, throughput, and Boot media (server booting from disk or the SAN). For example, maybe we require our virtual machines to support 3-4GB of memory with dual 4-Core CPUs. They will boot from the SAN. And the required LAN throughout would be 300Mbps and the SAN throughput would be 400Mbps.

Recommended

- **Network Adapter using CNA**: if you are using Cisco UCS C-series servers, it is recommended to use a network adapter that will support both Ethernet and Fibre Channel over Ethernet (FCoE). This will allow both data and storage traffic to share the same physical cabling (up to two 10-Gigabit Ethernet interfaces to a server). This is also called a Unified wire. This adapter should be used when the standalone server will be connected to either a Cisco Nexus 2232PP FEX (Data Center Access) or directly to the Cisco Nexus 5500UP (Data Center Core) for data and storage traffic. The Cisco Nexus 5500UP switch fabric would be responsible for splitting the FCoE traffic off to the Fibre Channel attached storage array. If FCoE will be used, the uplinks must use a fiber optic or Twinax connection to maintain the bit error rate (BER) thresholds for Fibre Channel transport.
- **Network Adapter using Fabric Extender (or IOM)**: if you are using a Cisco UCS B-series chassis server on the network. The Cisco UCS 2200 Series Fabric Extenders is like a mini fabric interconnect switch that exist within the Cisco UCS 5100 Series Blade Server Chassis with four 10GE/Fibre Channel ports. This module would then connect into a Fabric Interconnect switch. The Fabric Extenders would be responsible for extending the fabric from the interconnect switches to each chassis for Ethernet, FCoE, and management purposes. Only two IOM can exist in a single UCS chassis. Furthermore, Mezzanine Cards are used as virtual adapters to build a virtual NIC on the blade servers and bind them to the Fabric Extender for network connectivity.
- **Physical Servers based on High Performance**: the Cisco UCS server can support 24-96GB+ of memory with Dual 4-8 Core CPU. In this configuration, you could support up to 24 virtual machines with 4GB of memory. Or up to 32 virtual machines with 3GB of memory.
- **Physical Servers based on Medium Performance**: the Cisco UCS server can support 8-12GB of memory with Dual CPU or Dual 4-Core CPU. In this configuration, you could support up to 3 virtual machines with 4GB of memory. Or up to 4 virtual machines with 3GB of memory.
- **Physical Servers based on Standard Performance**: the Cisco UCS server can support 4-24GB of memory with a Single/Dual CPU. In this configuration, you could support up to 6 virtual machines with 4GB of memory. Or up to 8 virtual machines with 3GB of memory.
- **Power Calculation**: determine the power needed based on the Idle load and overall usage. This will include the load usage at 50% and the maximum usage at 100%.
- **End-Host Mode**: it is recommended to configure the Cisco Fabric Interconnect switches in “end-host” mode. This will allow the fabric interconnects to operate as transparent switches connecting up to the Data Center Core layer.

Optional	• **Network Adapter using HBA**: if the Cisco UCS C-series server will be connected directly into a Fibre Channel storage fabric (or SAN switch). • **Network Adapter using Cisco VICs**: used with Cisco UCS B-series servers to allow each virtual adapter to appear as a separate virtual interface on the fabric interconnects. It can support up to 256 total virtual interfaces split between the vNICs and vHBAs.

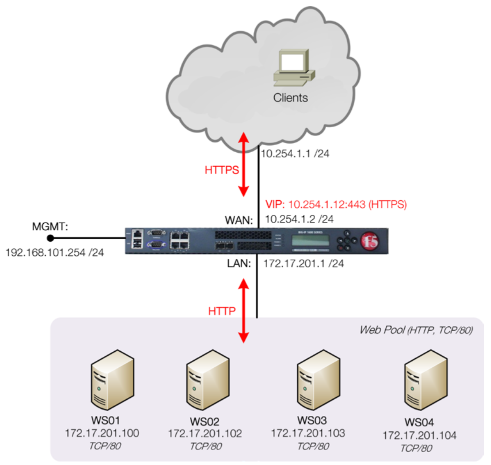
2.3 Load Balancing

Select one (or more) of the following Load Balancing PODs that will be used in the design:

	Local - Load Balancing	**Global – Load Balancing**

Local

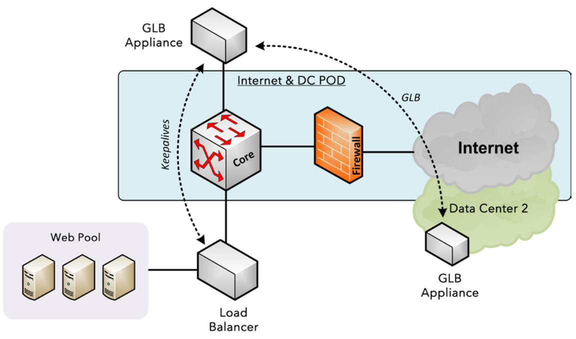
POD: LB-LOCAL



- **When to use**: if you require distribution of traffic across a group of servers for increased performance and availability
- **Prerequisites**: LB
- **Required**: --
- **Has Sub-PODs**: Go to 2.3.1

Global

POD: LB-GLOBAL



- **When to use**: if you require load balancing between sites in the event that a site goes down or the local load balancing resources are exceeded
- **Prerequisites**: LB, DC
- **Required**: --
- **Has Sub-PODs**: Go to 2.3.2

2.3.1 Local - Load Balancing

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for the local load-balancing solution:

Vendor Solutions	**F5 – BIG-IP LTM** If you require building a hardware-based load-balancing solution using F5 BIG-IP hardware. This is recommended for medium to large sized networks. There is a virtual edition and a physical appliance available.	**Citrix – NetScaler ADC** If you require building a hardware-based load-balancing solution using Citrix NetScaler hardware. This is recommended for medium to large sized networks. There is a virtual edition and a physical appliance available.
	Microsoft – NLB If you require building a software-based load-balancing solution supported on Microsoft Window servers. This is common for a small number of servers mainly due to cost. However, NLB has load balancing limitations that can affect overall performance and operations. NLB can support up to 32 servers (advertised) using HTTP.	**Radware - AppDirector** If you require building a hardware-based load-balancing solution using Radware's AppDirector OnDemand hardware platform. This is recommended for medium to large sized networks.

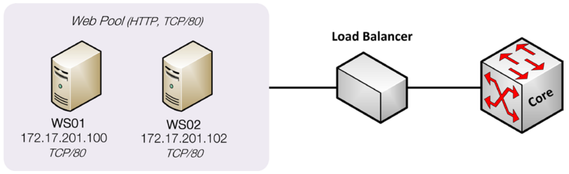
Deployments

Select one of the following load balancing deployments that will be used in the solution:

	In-Line Deployment	Out-of-Band Deployment

In-Line Deployment

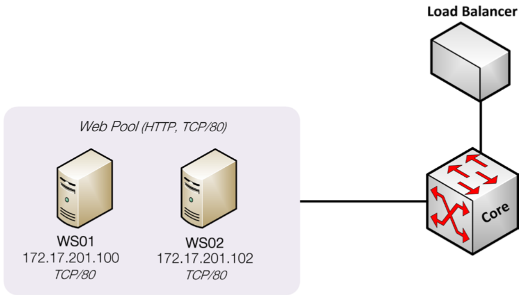
POD: LB-LOCAL-IL



- **When to use**: if you require deploying the LB appliance in-between the server farm and the rest of the data center. This POD is the most common over an OOB deployment.
- **Prerequisites**: LB-LOCAL
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: LB appliance, Servers
- **Description**: in this POD, the LB appliance uses two interfaces which is typically in-line between the server farm and the rest of the Data Center network. One interface (internal facing) connects to where the load-balanced server farm exists. And the other interface (external facing) connects to where client requests would be terminated to when accessing an application that will be load-balanced on the backend.

Out-of-Band Deployment

POD: LB-LOCAL-OOB



- **When to use**: if you require deploying the LB appliance using one interface connected into either the server farm or to the DC/LAN Core switch
- **Prerequisites**: LB-LOCAL
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: LB appliance, Servers
- **Description**: in this POD, the LB appliance uses a single interface connected to the Data Center Core (or within the Server Farm). This is the simplest deployment type to setup as it is not directly in the path of the traffic flow. It only receives traffic that is intended to be load balanced.

Configuration

Below are required, recommended, and optional configuration when deploying a local load-balancing solution on the network:

Required

- **Server Pool**: define the server pools that will be used within a server farm in the Data Center. Within each server pool determine the application and ports that should be load-balanced
- **Load Balancing Methods**: determine how the servers within the server pool will be load-balanced. The available options include Round Robin, Least Connections, Fastest Server, Ratio, etc.
- **Virtual Address**: for each server pool, determine the virtual address and port that will be used for how clients will access the server pool.

Recommended

- **Load Balancing using Least Connections**: each new client request is sent to the server that has the least number of connections. If the server hardware is the same, this method is recommended to ensure an even distribution of load balancing among the servers.
- **Health Monitors**: it's recommended for each server pool to be setup with a health monitor. This would periodically monitor each server within a pool to verify if the application is working. For example, if the HTTP services on a web server is turned off or has failed, the load balance appliance would put that server offline and will not use that server for load balancing within the pool. This provides reliability services for a server pool, so the client is always sent to a server that is available.

Optional

- **Persistence**: if you require the client to stay connected to the same server within a server pool. The available options include source IP address or using HTTP cookies.
- **Persistence using HTTP Cookies**: if you are using a web server farm
- **SSL Termination**: determine if SSL termination to the virtual address (and its server pool) on the load balance appliance is required. In this option, a single SSL certificate would be installed on the load balancer for a virtual address. Client requests would then be load balanced using HTTP requests to the local servers within the pool. The web servers in the pool do not require SSL certificates unless end-to-end server-side security is required. In this case, the load balance appliance would build a secure SSL tunnel with the client and each of the servers in the pool.

2.3.2 Global - Load Balancing

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for the global load balancing solution:

Vendor Solutions	**F5 – BIG-IP DNS** If you require building a hardware-based global load-balancing solution using F5 BIG-IP hardware. This is recommended for medium to large sized networks.	

2.4 Network Management

Select one (or more) of the following Network Management PODs that will be used in the design:

	Network Monitoring System (NMS)	**Deployment Management**	**Cloud Management**
	Security Management	**Desktop Management**	**Configuration Management**

NMS

POD: NM-NMS

- **When to use**: if you require monitoring the performance and faults located on the network or any of its devices
- **Prerequisites**: NM
- **Required**: OPS-SNMP, OPS-SYSLOG, OPS-NF
- **Has Sub-PODs**: Go to 2.4.1
- **Components**: NMS server(s)
- **Description**: this POD consists of one (or more) NMS platforms that is part of the server farm.

Deployment Management

POD: NM-DEPLOY

- **When to use**: if you require doing automated provisioning and configuration for a large group of identical servers
- **Prerequisites**: NM, DC
- **Required**: --
- **Has Sub-PODs**: Go to 2.4.2
- **Components**: Server(s)
- **Description**: this POD consists of one (or more) deployment management platforms that is part of the server farm to provide centralized configuration for the servers.

Cloud Management

POD: NM-CLOUD

- **When to use**: if you require management of cloud services used in the environment for easier administration
- **Prerequisites**: NM, COMP-CLD
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Server(s)
- **Description**: this POD consists of one (or more) cloud management platforms that is part of the server farm. Or it can be a cloud-based service that is used in the environment.

Security Management

POD: NM-SM

- **When to use**: if you require monitoring and management of all security aspects in the environment for auditing and troubleshooting purposes
- **Prerequisites**: NM, SEC
- **Required**: --
- **Has Sub-PODs**: Go to 2.4.3
- **Components**: Server(s)
- **Description**: this POD consists of one (or more) security management platforms that is part of the server farm.

Desktop Management

POD: NM-DTOP

- **When to use**: if you require using a desktop/laptop management system to manage patching, Anti-Virus, applications on the system, and tools for troubleshooting a problem on a desktop/laptop remotely
- **Prerequisites**: NM, LAN
- **Required**: --
- **Has Sub-PODs**: Go to 2.4.4
- **Components**: Server(s)
- **Description**: this POD consists of one (or more) desktop management platforms that is part of the server farm. Or it can be a cloud-based service that is used in the environment.

IP / Configuration Management

POD: NM-CFG

- **When to use**: if you require a system to manage the configuration and track changes made to the network devices. Other use-cases include IP address management (IPAM) for managing the allocation of IP addresses used in the environment.
- **Prerequisites**: NM, LAN
- **Required**: OPS-SNMP, OPS-SYSLOG
- **Has Sub-PODs**: --
- **Components**: Server(s)
- **Description**: this POD consists of one (or more) management platforms that is part of the server farm.

2.4.1 NMS

Complete each of the design sections below for the solution.

Vendor Solutions

Select one (or more) of the following vendors that will be used for the NMS solution.

Vendor Solutions	**Manage Engine** If you require fault and performance management of network devices using an on-site commercial solution	**Spiceworks** If you require fault and performance management of network devices using an on-site/cloud freeware solution
	PRTG Network Monitor If you require fault and performance management of network devices using an on-site commercial solution	**NetBrain** If you require automating network documentation and diagrams along with troubleshooting tools available
	What’s Up Gold If you require fault and performance management of network devices using an on-site commercial solution	**RouteHub - mBuilder** If you require fault management of network devices using a python web-based solution developed by RouteHub
	Cisco Prime Infrastructure If you require using a Cisco centric NMS product for fault and performance management of supported Cisco devices using an on-site commercial solution	

2.4.2 Deployment Management

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for deployment management:

Vendor Solutions	**Puppet** If you require using a deployment management tool that is aimed for system administrators working in heterogeneous network environments. Puppet uses a master-client model where a separate server is used for the master role and all servers that will be managed will be considered as clients.	**Chef** If you require using a deployment management tool that is aimed for developers who are familiar with Git and Ruby working in heterogeneous network environments. Chef uses a master-client model where a separate server is used for the master role and all servers that will be managed will be considered as clients.

2.4.3 Security Management

Complete each of the design sections below for the solution.

Vendor Solutions

Select one (or more) of the following vendors that will be used for security management:

Vendor Solutions	**Palo Alto Networks** To provide centralized management (called Panorama) of multiple Palo Alto Network firewall appliances for managing security policies, administration, reporting, and threat logs.	**Fortinet** There are several security management products for managing FortiGate firewall appliances. (1) FortiManager is used to provide centralized management of security policies and administration of multiple firewall appliances. (2) FortiAnalyzer is used to provide centralized log management for threats, logs, and reporting. (3) FortiCloud is used to provide cloud-based logs and reports. (4) SEIM is used to perform security audits and compliancy checks (HIPPA, SOX, PCI DSS).

2.4.4 Desktop Management

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for desktop management:

Vendor Solutions	**Kaseya - VSA** If you require central management of OS patching, Anti-Virus, monitoring, remote control, software patching, reporting, to scripting functionality for endpoint devices. Kaseya is the leader in the desktop management market.	**ConnectWise - Automate** If you require central management of OS patching, Anti-Virus, monitoring, remote control (called Screen Connect), software patching, reporting, to scripting functionality for endpoint devices. It also has integration with AutoTask and Manage ticketing systems.
	AutoTask – Endpoint Management If you require central management of OS patching, Anti-Virus, monitoring, remote control (called Splash Top), software patching, reporting, to scripting functionality for endpoint devices. It also has integration with the AutoTask ticketing system.	

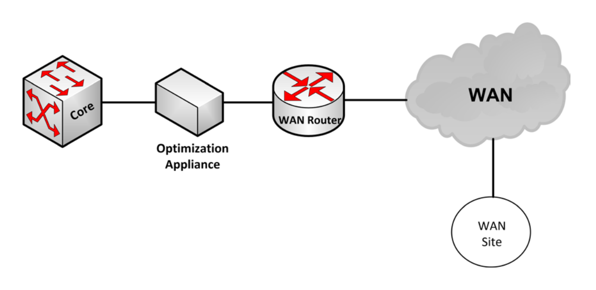
2.5 Optimization

Select one (or more) of the following optimization PODs that will be used in the design:

	WAN Optimization	

WAN Optimization

POD: OPT-WAN



- **When to use**: if you want to increase performance for user endpoints accessing applications (or data) over a WAN network with limited bandwidth resources
- **Prerequisites**: WAN
- **Required**: --
- **Has Sub-PODs**: Go to 2.5.1

2.5.1 WAN Optimization

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for the WAN optimization solution:

Vendor Solutions	**Riverbed – Steelhead** If you require building a hardware-based WAN optimization solution using Riverbed hardware. This is recommended for medium to large sized networks. There is a virtual edition and a physical appliance available.	**Silver Peak – NX / VX** If you require building a hardware-based WAN optimization solution using Silver Peak hardware. This is recommended for medium to large sized networks. There is a virtual edition and a physical appliance available.
	Cisco – WAAS If you require building a hardware-based WAN optimization solution using Cisco-based hardware. This is recommended for medium to large sized networks.	

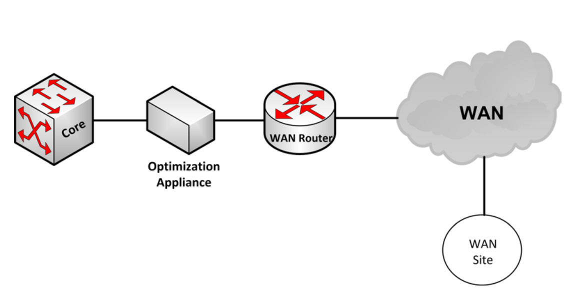
Deployments

Select one of the following WAN optimization deployments that will be used in the solution:

	In-Line Deployment	**Out-of-Band Deployment**

In-Line Deployment

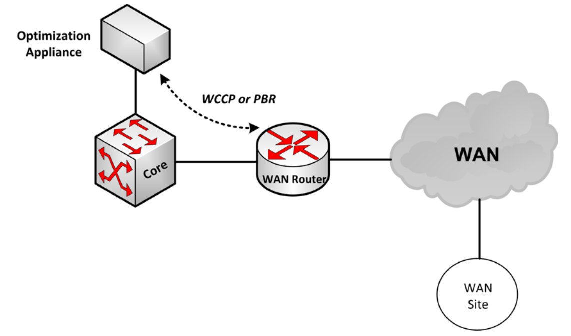
POD: OPT-WAN-IL



- **When to use**: if you require all traffic to be sent to the appliance for WAN optimization. This is ideal for remote sites. This deployment is most commonly used for WAN optimization.
- **Prerequisites**: OPT-WAN, Vendor (Any)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: WAN optimization appliance
- **Description**: in this POD, the WAN appliance uses two interfaces which is typically in-line between the WAN cloud and the LAN/DC network.

Out-of-Band Deployment

POD: OPT-WAN-OOB



- **When to use**: if you don’t require all traffic to be sent to the appliance for WAN optimization. This is ideal for Data Centers which only needs to optimize traffic to the remote sites.
- **Prerequisites**: OPT-WAN, Vendor (Any)
- **Required**: OPS-WCCP
- **Has Sub-PODs**: --
- **Components**: WAN optimization appliance
- **Description**: in this POD, the WAN appliance uses a single interface connected to either the LAN/DC Core switch or directly with the WAN router. WCCP would be used for redirecting traffic to the WAN appliance for traffic optimization.

Configuration – Riverbed Steelhead

Below are required, recommended, and optional configuration when deploying a Riverbed Steelhead WAN optimization solution on the network:

Required

- **Interfaces**: define all of the interfaces that will be used on the WAN optimization appliance. They include the LAN facing interface which will connect into the LAN/DC Core switch. There is the WAN facing interface which will connect to the WAN cloud (or WAN router). There is the Primary interface which is used for managing the appliance and would be plugged into a management VLAN on the LAN/DC. And there is a logical interface (in_path) which is used for auto-discovery, peering with other appliances across the WAN, and for traffic optimization.
- **Choosing Hardware**: for each optimization appliance that will be used on the network, select the best hardware model based on the business size, office type (branch office, Data Center), number of concurrent TCP connections, WAN bandwidth, and the data store size.
- **Optimization Mechanisms**: determine all of the optimization mechanisms that will be used on the appliance to learn and optimize traffic over slow networks. This will include Data, Transport, Application, and Management streamlining.
- **Auto Discovery**: used to locate remote Steelhead appliances in order to optimize traffic between them. There is basic and enhanced auto discovery.
- **In Path & Peering Rules**: it is important to setup rules between the client-end and the server-end appliances to signify what subnets (or traffic) should be optimized over the WAN.

Recommended

- **Optimization Mechanism using Data Streamlining**: this is recommended to provide data compression techniques including a proprietary algorithm called Scalable Data Referencing (SDR) to increase performance. SDR's primary function is to reduce the amount of WAN bandwidth (up to 99%) to provide fast data transfers.
- **Optimization Mechanism using Transport Streamlining**: this is recommended to provide efficient delivery of TCP packets over a WAN (or slow network) and improving the TCP slow-start process. This mechanism can also limit the number of TCP requests between the client and the server which will reduce the amount of TCP activity over the WAN.
- **Optimization Mechanism using Application Streamlining**: this is recommended to learn about application conversations that occur for its normal operation. It can minimize chatty application traffic over the WAN such as CIFS and Microsoft Exchange MAPI applications. Other applications can include HTTP, HTTPS, IMAP, NFSv3, and Oracle.
- **Optimization Mechanism using Management Streamlining**: this is recommended to provide auto discovery which is used to find remote Steelhead appliances in order to optimize traffic between them.
- **Auto Discovery using Enhanced**: allows the Steelhead appliance on the client-end to discover the last Steelhead appliance along the path to the server-end. If there are 3 or more appliances, then the last one, on that path would be discovered and used as the remote-end peer. Enhanced Auto Discovery can continue to operate if basic discovery is enabled on the other end, but it is not default. However, it is recommended to keep everything consistent with the Steelhead appliances that you deploy.

Optional

- **Auto Discovery using Basic**: if there are only two Steelhead appliances along the path between the client-end and the server-end. It is recommended to implement Enhanced Auto Discovery instead.

2.6 Security

Select one (or more) of the following security PODs that will be used in the design:

🟨	**General Security**	**Network Security**	**Application Security**	**Endpoint Security**	**Cloud Security**

There are many security mechanisms available to protect networks, applications, to endpoints. It will depend on how much security is required for your network. There are two levels of security enforcement:

Security Level 1 (Static): the first security level is the most common and provides static security protection. This involves using next-generation firewalls, endpoint security, to application security products. Static security deals with blocking known threats based on threat signatures, categories, or IP addresses found in a block list. The table below shows all of the security POD's used to provide level 1 security. It is really broken up into sub-levels based on what the firewall supports. Most environments use security at level 1.2 which involves deploying a next-generation firewall enabled for several security features. Implementing all of level 1 provides stronger security. For example, incoming traffic will first check the reputation (1.1) of the source and block if needed. Next, (1.2) the next-generation firewall appliance will inspect the traffic against several filters. And lastly, (1.3) additional security can be added directly to the applications and endpoints that are used.

1.0	**1.1**	**Network Security**: Firewall – Security Feature: Reputation	
	1.2	**Network Security**: Firewall – Security Features: Application Control, Web/URL Filtering, Anti-Virus, IPS, DoS Protection, File Blocking, Data Filtering, SSL/TLS Decryption	
	1.3	**Application Security**	**Endpoint Security**

Security Level 2 (Dynamic): the second security level provides dynamic security protection. This provides an advanced level or deeper inspection for known and zero day (real-time) threats. This means, learning the behavior of traffic from the security products at the first security level. It can also sandbox some of the traffic for deeper analysis on how dangerous it can be such as malware variants. If it determines that it is a new undefined threat, it can inform the first security level products to block the new threat. Furthermore, it will send the new threat info to it vendors threat research team (in the cloud) so it can be crafted as a new signature then updated to all security appliances, everywhere. Implementing Advanced Threat Protection would be the second level of security that can be enforced in the environment:

2.0	**Network Security**: Advanced Threat Protection

Therefore, determine what level 1 (and/or level 2) security PODs should be used in the design.

Network Security

Select one (or more) of the following Network Security PODs that will be used in the design:

Firewall	**VPN & Remote Access**	**Identity Control**
Encryption	**Advanced Threat Protection**	

Firewall

POD: SEC-NET-FW

- **When to use**: if you require restricting traffic to or from one (or more) network
- **Prerequisites**: INET
- **Required**: NAT
- **Has Sub-PODs**: Go to 2.6.2

VPN & Remote Access

POD: SEC-NET-VPN

- **When to use**: if you require either (1) a solution where users from the Internet can access network resources remotely. And/or (2) connecting with other sites over the Internet and not using a WAN cloud
- **Prerequisites**: INET
- **Required**: --
- **Has Sub-PODs**: Go to 2.6.3

Identity Control

POD: SEC-NET-ID

- **When to use**: if you require filtering traffic or applying unique security policies based on a user group or identity pulled from Active Directory (or LDAP)
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 2.6.4

Encryption

POD: SEC-NET-ENC

- **When to use**: if you require SSL decryption services and/or encryption services used on the network to provide data confidentiality and integrity
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 2.6.5

Advanced Threat Protection

POD: SEC-NET-ATP

- **When to use**: if you require an advanced level of deep inspection for known and zero day (real-time) threats
- **Prerequisites**: SEC-NET-FW
- **Required**: --
- **Has Sub-PODs**: Go to 2.6.6

Application Security

Select one (or more) of the following Application Security PODs that will be used in the design:

	Web Security	**Mail Security**	**DNS Security**
	Remote Desktop Security		

Web Security

POD: SEC-APP-WEB

- **When to use**: recommended services to provide security protection for web applications used in the environment
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 2.6.7

Mail Security

POD: SEC-APP-MAIL

- **When to use**: recommended services to provide security protection for mail applications used in the environment
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 2.6.8

Remote Desktop (RDP) Security

POD: SEC-APP-RDP

- **When to use**: recommended services to provide security protection for remote desktop services used in the environment
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 2.6.9

DNS Security

POD: SEC-APP-DNS

- **When to use**: recommended services to provide security protection for DNS services used in the environment
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 2.6.10

Additional Security

Select one (or more) of the following PODs that will be used in the design:

	General Security	**Endpoint Security**	**Cloud Security**

General Security

POD: SEC-GEN

- **When to use**: this is recommended for implementing general security along with other best practices for the network devices in the environment
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 2.6.1

Endpoint Security

POD: SEC-END

- **When to use**: if you require implementing security services to all endpoints connected to the network which includes desktops, servers, to mobile devices
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 2.6.11

Cloud Security

POD: SEC-CLD

- **When to use**: if you require providing additional security for cloud-based applications (SaaS) that are used in the environment
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 2.6.12

2.6.1 General Security

Select one (or more) of the following general security practices that will be used:

	Security Policy	**Security Standards**	

Security Policy
POD: SEC-GEN-POL
• **When to use**: to provide a general policy of security requirements and recommendations in the environment • **Prerequisites**: -- • **Required**: SEC2-GEN • **Has Sub-PODs**: Go to 2.6.1.1

Security Standards
POD: SEC-GEN-STD
• **When to use**: if you require following security practices (or regulatory compliancy) outlined in FIPS, ANSI, or PCI • **Prerequisites**: SEC-GEN-POL • **Required**: NM-SM, SEC2-GEN • **Has Sub-PODs**: Go to 2.6.1.2

2.6.1.1 Security Policy

Below are recommendations to include in the information security policy:

Services	**Passwords** Use strong passwords or phrases containing capital letters, numbers, and special characters. Do not share passwords with other people (internal or external).	**Two Factor Authentication** This provides strong password security using two level of passwords. The first level involves using a static password that is created by the user. The second level involves using a time-based temporary passcode that will be visible in a security token. This is highly recommended for highly-sensitive systems to protect against brute-force attacks.
	Computer Security To prevent unauthorized access to computer systems, make sure to log out when finished. Use a password-protected screen saver. It is also recommended to use a security cable to lock the laptop/computer system.	**Documents** Do not leave documents unattended on a copier or fax machine. Use shredding bin for any confidential documents that need to be discarded. All confidential documents that are not in use should be filed away in a lockable cabinet.
	Email Policy Do not create/forward offensive messages about age, gender, sexual orientation, race, ethnicity, religion, pornography, chain letters, hoaxes or political beliefs. Do not send sensitive information such as credit card numbers, SSN, to account numbers.	**On-line Fraud & Phishing** This threat deals with stealing identities that can be used for on-line fraud. Phishing is basically a decoy email that looks legit aimed to get personal information. Do not follow links in an email to visit any site that is asking you to log in. Instead, type in the website address into your web browser to get to the required website.
	Identity Theft This ideals with someone stealing and using a person's information. Do not give any personal information over the phone nor email to unknown persons.	**Change Control** Any configuration change that must be completed on any network device must be reviewed and approved before applying. This can lower the chance of user error that can cause an outage. Having a change control process can help others to understand what changes are being made and how to revert back if necessary.
	Documentation Creating documentation and keeping it updated is very important for understanding how your network is designed. This is good for troubleshooting purposes including planning like adding a new network solutions. Documentation is also important plus mandatory when a company follows a particular compliancy such as SOX or HIPPA. Network documentation can include: Network Diagrams and Contact List (Vendors, Providers).	

2.6.1.2 Security Standards

Below are security standards that can be used:

Standards	**PCI/DSS** Required compliancy if the company network deals with credit card processing	**FIPS** Security best practices of encryption and random password generation used for US Government network environments
	ANSI Security best practices of encryption and authentication of financial transactions used for US banking network environments	

Deployment - PCI / DSS

Below are the 12 PCI requirements for network implementation to be PCI compliant:

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored data.
4. Encrypt transmission of cardholder data and sensitive information across public networks.
5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

2.6.2 Firewall

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for the firewall solution:

Combined / Standalone	**Palo Alto Networks - NGFW** If you require using a medium to large enterprise firewall solution using Palo Alto Networks hardware to provide advanced next-generation security	**Fortinet – FortiGate** If you require using an enterprise firewall solution using FortiGate hardware to provide advanced next-generation security
	Cisco – ASA FirePOWER If you require using an enterprise firewall solution using Cisco ASA Firepower hardware to provide advanced next-generation security	**Check Point – Enterprise, SMB** If you require using an enterprise firewall solution using Check Point hardware to provide advanced next-generation security
	SonicWALL If you require using a small to SMB enterprise firewall solution using SonicWALL hardware to provide advanced next-generation security	**Juniper - SRX** If you require using an enterprise firewall solution using Juniper SRX hardware to provide advanced next-generation security.

Integrated	**Access Control List (ACL)** If you require implementing basic firewall services on one (or more) of the existing Layer-3 network devices in the environment such as the Core switch, edge router, and/or WAN router.	

Deployment

Select all of the PODs that will be used for the solution:

	Firewall Deployment	**Security Features**	

Firewall Deployment

POD: SEC-NET-FW-DEPLOY

- **When to use**: this is required to determine how the firewall solution will be deployed
- **Prerequisites**: SEC-NET-FW
- **Required**: --
- **Has Sub-PODs**: Go to 2.6.2.1

Security Features

POD: SEC-NET-FW-FEAT

- **When to use**: this is required to determine what security features will be implemented on the firewall appliance
- **Prerequisites**: SEC-NET-FW-DEPLOY-STD, SEC-NET-FW-DEPLOY-HA1, SEC-NET-FW-DEPLOY-HA2, SEC-NET-FW-DEPLOY-INTG3
- **Required**: --
- **Has Sub-PODs**: Go to 2.6.2.2

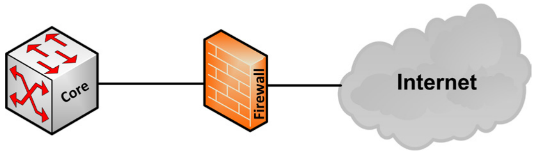
2.6.2.1 Firewall Deployment

Select one (or more) of the following PODs for how the firewall appliance will be deployed:

	Standalone NGFW	**FW/ACL on Internet Edge**	**FW/ACL on LAN/DC**
	NGFW on LAN/DC	**NGFW Redundancy (Active/Passive)**	**NGFW Redundancy (Active/Active)**

Standalone NGFW

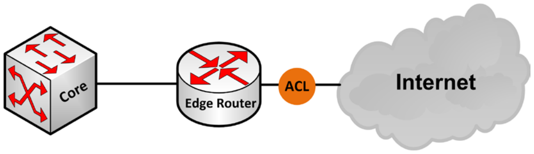
POD: SEC-NET-FW-DEPLOY-STD



- **When to use**: if you require deploying a firewall appliance to provide security protection for one (or more) trusted internal networks such as the LAN and Data Center. This is recommended for the firewall solution if it will be connected to the Internet.
- **Prerequisites**: SEC-NET-FW-DEPLOY, Vendor (Combined/Standalone)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Firewall appliance
- **Description**: in this POD, a next-generation firewall appliance will be deployed in-line between a trusted network (LAN, DC) and an untrusted network (Internet), as shown in the picture above, enabled with various security features.

FW/ACL on Internet Edge

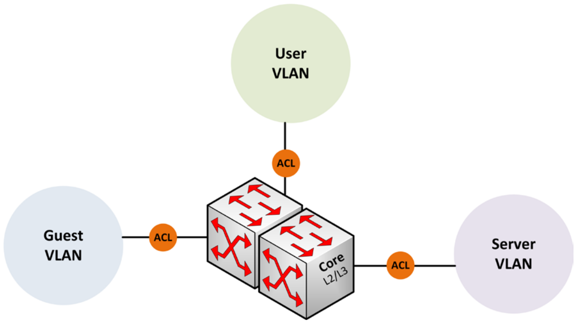
POD: SEC-NET-FW-DEPLOY-INTG1



- **When to use**: if you require using the Internet edge router for basic firewall services without using a firewall appliance
- **Prerequisites**: SEC-NET-FW, Vendor (Integrated)
- **Required**: SEC2-ACL-INET
- **Has Sub-PODs**: --
- **Components**: Edge router
- **Description**: in this POD, ACL services are configured on the Internet edge router acting as a basic Stateful firewall as shown in the picture above. No firewall appliance is required; however, only basic firewall services are supported.

FW/ACL on LAN/DC

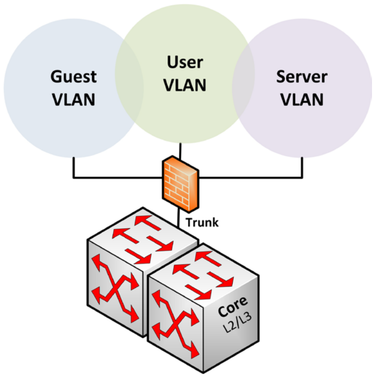
POD: SEC-NET-FW-DEPLOY-INTG2



- **When to use**: if you require basic filtering between VLANs on the LAN (or Data Center)
- **Prerequisites**: SEC-NET-FW, Vendor (Integrated)
- **Required**: SEC2-ACL-LANDC
- **Has Sub-PODs**: --
- **Components**: Core switch
- **Description**: in this POD, ACL services are configured on the Core switch within the LAN/DC. ACL rules are configured on the Layer-3 VLANs interfaces (SVI) to restrict communication between the VLANs (e.g. User VLAN, Server VLAN, Guest VLAN) as shown in the picture above. Only basic firewall services are supported.

NGFW on LAN/DC

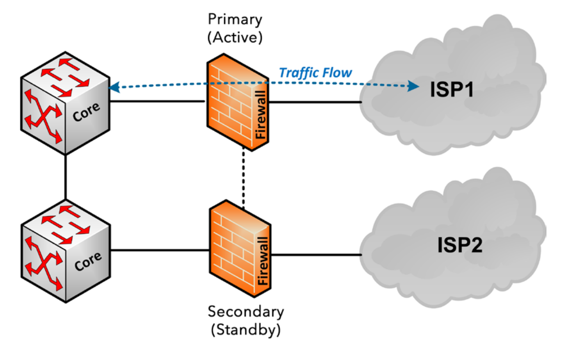
POD: SEC-NET-FW-DEPLOY-INTG3



- **When to use**: if you require advanced filtering (e.g. URL, Application, Malware, IPS) between VLANs on the LAN (or Data Center)
- **Prerequisites**: SEC-NET-FW, Vendor (Combined/Standalone)
- **Required**: SW
- **Has Sub-PODs**: --
- **Components**: Core switch, Firewall appliance
- **Description**: in this POD, a firewall appliance is connected directly on the Core switch. 802.1Q Trunking would be configured between the Core switch and firewall appliance for the VLANs (e.g. User VLAN, Server VLAN, Guest VLAN) you want to secure as shown in the picture above. This will allow restricting traffic and providing advanced security protection for those secure VLANs.

NGFW Redundancy (Active/Passive)

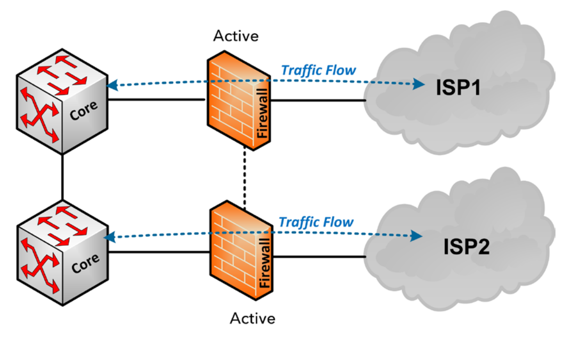
POD: SEC-NET-FW-DEPLOY-HA1



- **When to use**: if you require high-availability with the firewall solution and want one firewall appliance to be active while the other is in standby mode ready to take over
- **Prerequisites**: SEC-NET-FW
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Firewall Appliances
- **Description**: in this POD, two firewall appliances are connected in-line between the two networks you want to protect which will typically be the Internet and the LAN/DC as shown in the picture above. One (or more) connections would exist between the firewalls to exchange state information and configuration. In an active/passive configuration, one device is active while the other device is in standby monitoring the operational status of the primary device and ready to transparently takeover if a failure occurs.

NGFW Redundancy (Active/Active)

POD: SEC-NET-FW-DEPLOY-HA2



- **When to use**: if you require high-availability with the firewall solution and want both firewall appliances to be actively running at the same time
- **Prerequisites**: SEC-NET-FW
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Firewall Appliances
- **Description**: in this POD, two firewall appliances are connected in-line between the two networks you want to protect which will typically be the Internet and the LAN/DC as shown in the picture above. One (or more) connections would exist between the firewalls to exchange state information and configuration. In an active/active configuration, both firewalls are active at the same time providing both redundancy and load balancing capabilities.

Configuration

Below are required, recommended, and optional configuration when deploying a firewall appliance on the network:

Required

- **Layer-3 Mode**: determine how the firewall appliance will be deployed in-line between the two networks. The available options are Layer-2 mode and Layer-3 mode. The most common type (and the default) of a firewall deployment is using Layer-3 mode.
- **Security Policies**: firewall policies are required for what should be allowed inbound and outbound between the various network zones (e.g. Trusted, Untrusted, DMZ). Determine what services require direct inbound access from the untrusted network and only allow those services with an inbound policy. For outbound filtering determine if a whitelist policy (recommended) and/or blacklist policy (optional) will be used.
- **Application Categories**: define the application categories that should be blocked.

Recommended

- **Whitelist Security Policy**: this policy structure is recommended for environments that want to provide a higher level of security or have regulatory requirements. Whitelist policy rules will block all outbound traffic except for specific applications/services should be allowed. The default action in a whitelist policy would be to "***deny all***" traffic.
- **Security Policies for RFC1918**: rules that should be added to an inbound access policy to filter any private IP addresses sourced from the Internet which should only consist of Public IP addresses.
- **Security Policies for RFC2827 (Anti-Spoofing)**: rules that should be added to an inbound access policy to filter any source IP addresses that should only exist behind the firewall/trusted environment. For example, let's say that the trusted network is using the 4.4.4.0 subnet. Any communication from that Public subnet should only be the source for outbound connections. For inbound connections, it should appear in the destination field. If a new IP connection comes into the Public facing interface of the firewall/router and see's that the source is 4.4.4.X then the connection is likely being spoofed in some type of attack. Hence, that connection should be blocked.
- **Security Policies for SMTP**: configure a rule to allow SMTP outbound access from a set of authorized SMTP servers. This ensures that SMTP related attacks caused by infected computers don't send large amounts of SPAM messages from the network causing network congestion. It can also potentially blacklist an email server for a company that uses a fixed IP address (common for small and SMB sized networks).
- **Security Policies for DNS**: configure an inbound rule to allow DNS on UDP port 53 if there will be an internal DNS server that will be accessed from the Internet. Furthermore, it is recommended to block DNS on TCP port 53 if zone transfers between authoritative name servers is not required. Opening DNS on TCP/43 can allow hackers to perform reconnaissance attacks to learn about the network environment to do further damage.
- **Inspection for Real-Time Applications**: if SIP (or H.323) traffic will be flowing through the firewall appliance, it is recommended to disable application inspection for those real-time applications so SIP traffic can operate correctly.

Optional	• **Blacklist Security Policy**: this policy structure is the simplest to maintain for environments over whitelist policy rules. Blacklist policy rules will block outbound access for specific applications/services that poses the greatest risk to the internal network. The default action in a blacklist policy would be to “***permit all***” traffic. • **Layer-2 Mode**: if you require adding the firewall appliance between other networks without re-addressing the hosts and/or network devices. • **Virtualization**: if you require the firewall appliance to be partitioned (or virtualized) on the same physical firewall. Common for hosted networks with clients using a virtualized firewall. This would be considered as a type of NFV that can be used. • **Rate Limiting / Traffic Shaping**: if you require rate limiting/shaping traffic to a specific bandwidth rate for a user or security policy. • **Security Policies for Applications (Non-Business):** it’s recommended to block any application for any category not considered business relevant such as social networking (e.g. Facebook, Twitter).

2.6.2.2 Security Features

Select one (or more) of the following security features that will be implemented on the firewall appliance:

Security Features	**Application Control** If you require filtering traffic based on the actual applications that are used in the environment for deeper inspection	**Intrusion Prevention (IPS)** If you require deep-level inspection of traffic coming in and out of the network for known threats or exploits including ransomware
	Web / URL Filtering If you require filtering traffic based on the URL and high-risk/inappropriate website category content on the Internet	**Anti-Virus, Anti-Bot** If you require filtering traffic for malware, bots, viruses, and ransomware detected
	File Blocking If you require allowing certain file types and/or inspecting files for known threats	**Data Filtering** If you require scanning files for credit card (CC) numbers, social security numbers (SSN), to certain data patterns encountered
	SSL/TLS Decryption If you require decrypting secure web pages for further inspection of threats and exploits. This operation is accomplished when the firewall intercepts a secure session initiated by an internal user. In return, the secure tunnel is now established between the destination site and the firewall acting on behalf of the client. Furthermore, the firewall builds another secure tunnel with the user.	**Reputation** If you require proactive security by filtering traffic based on known domains and IP addresses with poor reputations associated with malicious activity
	DoS / DDoS Protection If you require adding an additional layer of security to prevent against DoS/DDoS attacks into the network. These attacks can include port scans, floods, sweeps/discovery, and other DoS related threats.	

Configuration - General

Below are required, recommended, and optional configuration when implementing security features on the firewall appliance:

Required

- **Subscription & Licensing**: make sure to activate and license all security features that will be configured on the firewall appliance to receive the most recent attack signatures and updates.
- **Allowed / Blocked File Types**: determine what file types should be allowed (or blocked) on the firewall appliance.
- **Reputation List**: based on the vendor solution, determine how the reputation list will be obtained in which the firewall appliance will look at first before going through the configured security policies. This may be a list of IP address, domains, and/or URLs provided by the vendor (recommended) or an external list managed by a third-party source.
- **IPS Mode**: determine the IPS mode that will be used. The available options include Active (Block) and Passive (Monitor only) Modes.
- **Certificate for SSL/TLS Decryption (Deep Inspection):** user endpoints must trust the certificate generated on the firewall appliance using either group policies (GPO) and/or manually importing the certificate into the user's web browsers to avoid receiving a security warning.

Recommended (1/2)

- **Block security risk categories**: it's recommended to detect and block content for malicious sites, phishing, spyware, anonymizers, proxies, hacking, Spam URLs, Malware, Botnets, C2 (C&C), TOR (dark web), Bogon and any other critical/high security risk categories for all security features implemented.
- **Block inappropriate content categories**: it's recommended to block content for adult/mature websites such as pornography including violence, illegal activities, drugs, racism, hate, etc.
- **Block file sharing (and bandwidth consuming) categories**: it's recommended to block content for P2P and BitTorrent applications.
- **Block Categories for Public facing Servers**: If there will be servers accessed from the outside, it is recommended to enable critical/high severity + server-based threats for IPS signatures based on the applications (e.g. HTTP, FTP) that are used. Those IPS signatures should be set to block for any application attack that occurs to that inbound server.
- **IPS Active Mode (Block):** the IPS engine will inspect all traffic on the network. If there is any type of attack or malicious activity it will proactively block the connection. This offers greater security protection for preventing attacks on the network.
- **Executable File Types**: it's recommended to block executable file types
- **Data Filtering for CC & SSN**: it is recommended to scan and block files containing credit card (CC) numbers and social security numbers (SSN) being uploaded/download in the environment.
- **Events and Alerting**: confirm the appropriate action to take if an attack is discovered such as receiving alerts via email, SMS messages, and/or generating a log event that can be viewed on the firewall appliance.

Recommended (2/2)

- **Dynamic Block Lists**: it is recommended to use a block list of IP addresses, domains, and URLs maintained by the vendor such as Cisco with its Security Intelligence feed. Using third-party block lists may not be regularly updated (or trusted) to add new IP addresses (or domains) with poor reputations.
- **Web Categories for SSL/TLS Decryption**: it is recommended to decrypt malicious (or high risk) site categories for deeper inspection. Decrypting web-sites that contain private information such as banking or financial sites are typically excluded from SSL inspection.

Optional

- **Block non-business categories**: it's recommended to block content for any web category not considered business related such as social networking (e.g. Facebook, Twitter), video (YouTube, Netflix), to web-based email (e.g. Gmail, Outlook).
- **URL Filtering based on Individuals**: if you require creating a web security policy unique for certain individuals that is different from other groups.
- **URL Filtering based on Subnets (or Groups):** if you require a web security policy for an entire subnet (or group).
- **Data Filtering for Data Patterns**: if you want to scan and block files that contain certain patterns based on a security requirement from being uploaded/download in the environment.
- **IPS Passive Mode (Monitor):** in this mode, the IPS/IDS engine will only inspect traffic on the network and if there is any type of an attack it will only report back to the management server, send a log, and/or send an email to the security administrator. This is also called “promiscuous mode”.

Configuration – DoS Protection

Below are required, recommended, and optional configuration when deploying DoS protection on the network:

Required

- **DoS Mechanisms**: determine the DoS protection mechanism(s) that will be enabled on the security appliance (standalone or combined). They can include flood protection (TCP SYN, ICMP, UDP), reconnaissance protection (port scan), and IP Packet based protection.

Recommended

- **DoS Mechanism using Flood Protection**: this is recommended to be enabled to protect against TCP SYN, ICMP, and UDP flood attacks. For TCP SYN flood protection you can enable either Random Early Drop (default) or SYN Cookies (recommended if supported). RED is the most common mechanism supported to provide protection for TCP SYN, ICMP, and UDP packets. SYN Cookies is supported to provide protection for TCP SYN packets only. Flood protection should be configured to generate an alert, active RED (or SYN Cookies) operations, and define a maximum threshold when a certain number of packets per second (pps) has been reached.
- **DoS Mechanism using Reconnaissance Protection**: this is recommended to be enabled to protect against port scans, host sweeps, and UDP scans.
- **DoS Mechanism using Packet based Protection**: this is recommended to be enabled to protect against IP spoofing, fragmented traffic, mismatched TCP segments, and rejecting non-SYN TCP packets. It is also recommended to block IP packets with certain IP options set such as strict source routing, loose strict routing and record route. These options could be used to change the routing path to evade security measures. Other IP packet based protections for ICMP include blocking ICMP fragments and ICMP packets larger than 1KB.

Optional

- **Flood Protection using Small Session Tables**: if you require the security appliance to keep a small session table for all TCP sessions established through the firewall. This is accomplished by setting the thresholds to alert if there are 10,000 SYN packets per second. It would also activate the SYN Cookies/RED operations when the first TCP SYN message arrives. And the maximum number should be set to 1 million packets per second. Using this approach will increase the CPU usage on the security appliance.
- **Flood Protection using Large Session Tables**: if you require the security appliance to keep a large session table for all TCP sessions established through the firewall to keep the CPU usage low. This is accomplished by setting the thresholds to alert if there are 10,000 SYN packets per second and it would also activate the SYN Cookies/RED operations at the same time. The maximum number would be set to 1 million packets per second.
- **Flood Protection based on Average Sessions**: this is recommended if you understand the average number of TCP sessions stored in the session table. This is accomplished by setting the thresholds to alert at 10% of the average number of sessions. The SYN cookies/RED activation would be 10% of the alert value. And the maximum threshold would be 30% of the activate value. For example, if the average number of session is 5000, the alert would be 5300 packets per second. SYN cookies/RED operations would be activated at 5800 packets per second. And the maximum number would be 7500 packets per second.

2.6.3 VPN & Remote Access

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for VPN and/or remote access:

Combined / Standalone	**Palo Alto Networks - NGFW** If you require deploying VPN services on a standalone Palo Alto Networks firewall appliance. Or deploying VPN services on the existing firewall appliance with other security features enabled (e.g. FW, IPS, URL).	**Fortinet – FortiGate** If you require deploying VPN services on a standalone FortiGate firewall appliance. Or deploying VPN services on the existing firewall appliance with other security features enabled (e.g. FW, IPS, URL).
	Cisco – ASA FirePOWER If you require deploying VPN services on a standalone Cisco ASA Firepower firewall appliance. Or deploying VPN services on the existing firewall appliance with other security features enabled (e.g. FW, IPS, URL).	**Check Point – Enterprise, SMB** If you require deploying VPN services on a standalone Check Point firewall appliance. Or deploying VPN services on the existing firewall appliance with other security features enabled (e.g. FW, IPS, URL).
	SonicWALL If you require deploying VPN services on a standalone SonicWALL firewall appliance. Or deploying VPN services on the existing firewall appliance with other security features enabled (e.g. FW, IPS, URL).	**Juniper - SRX** If you require deploying VPN services on a standalone Juniper SRX security appliance. Or deploying VPN services on the existing firewall appliance with other security features enabled (e.g. FW, IPS, URL).

Integrated	**VPN Services on Router** If you require implementing VPN services on one (or more) of the existing network devices such as the Edge or WAN Routers in the topology. This is used to support advanced VPN technologies such as DMVPN and GET VPN.	

Deployment

Select all of the PODs that will be used for the solution:

	VPN Type	**Appliance Deployment**	

VPN Type

POD: SEC-NET-VPN-TYPE

- **When to use**: this is required to determine the type of VPN solution that is required in the environment
- **Prerequisites**: SEC-NET-VPN
- **Required**: SEC-NET-VPN-DEPLOY
- **Has Sub-PODs**: Go to 2.6.3.1

VPN Deployment

POD: SEC-NET-VPN-DEPLOY

- **When to use**: this is required to determine how the VPN solution will be deployed
- **Prerequisites**: SEC-NET-VPN-TYPE
- **Required**: --
- **Has Sub-PODs**: Go to 2.6.3.2

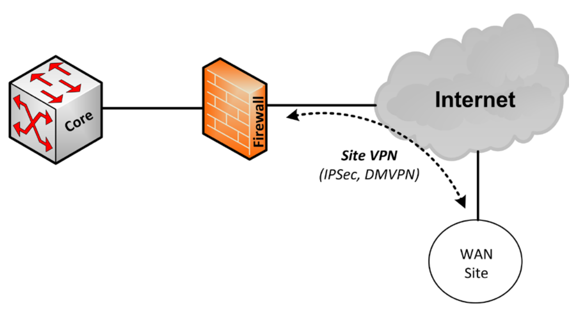
2.6.3.1 VPN Type

Select one (or more) of the following PODs that will be used:

🟩	**Site-to-Site VPN**	**Client VPN (Remote Access)**	

Site-to-Site VPN

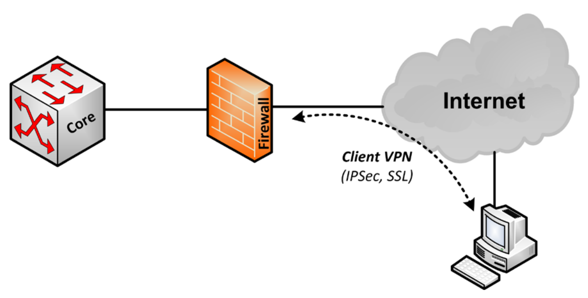
POD: SEC-NET-VPN-SVPN



- **When to use**: if you require building a permanent secure tunnel between two (or more) locations over the Internet (or WAN)
- **Prerequisites**: SEC-NET-FW-TYPE
- **Required**: --
- **Has Sub-PODs**: Go to 2.6.3.3
- **Components**: VPN appliance
- **Description**: in this POD, the VPN appliance would be connected to the Internet and the LAN/DC. It would build one (or more) secure VPN tunnels with other VPN appliances as shown in the picture above.

Client VPN (Remote Access)

POD: SEC-NET-VPN-CVPN



- **When to use**: if you require building a remote access solution where users can access network resources remotely using a VPN client program
- **Prerequisites**: SEC-NET-FW-TYPE
- **Required**: --
- **Has Sub-PODs**: Go to 2.6.3.4
- **Components**: VPN appliance
- **Description**: in this POD, the VPN appliance would be connected to the Internet and the LAN/DC where the network resources would be located as shown in the picture above. The users would connect to the VPN appliance using the IP address of the WAN facing interface on the appliance.

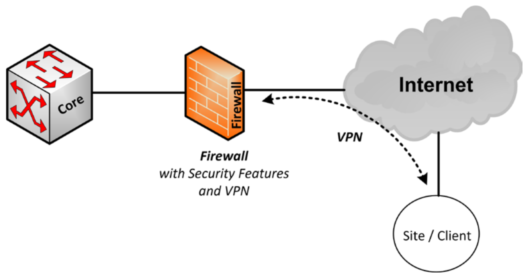
2.6.3.2 VPN Deployment

Select one of the following deployments that will be used for the VPN solution:

🟩	**Combined Deployment**	**Standalone Deployment**	**Integrated Deployment**

Combined Deployment

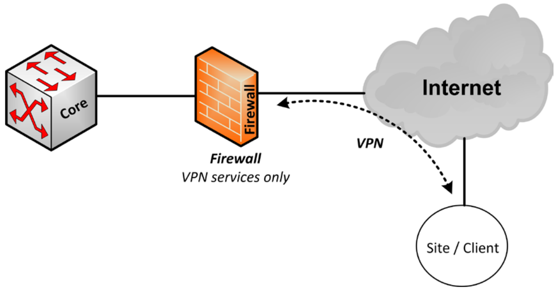
POD: SEC-NET-VPN-DEPLOY-COMB



- **When to use**: if you require (or prefer) VPN services to be enabled on the firewall appliance along with other security features enabled such as IPS and URL. This is used if there will be a moderate number of VPN connections.
- **Prerequisites**: SEC-NET-FW, SEC-NET-VPN, Vendor (Combined)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Firewall appliance
- **Description**: in this POD, VPN services would be enabled on the existing firewall appliance in the environment as shown in the picture above.

Standalone Deployment

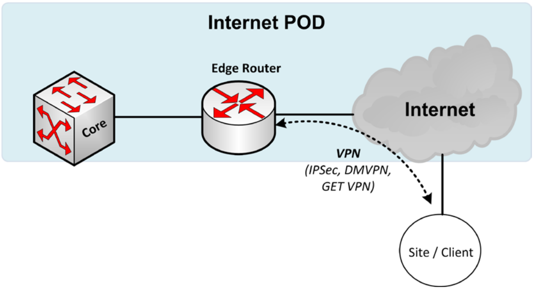
POD: SEC-NET-VPN-DEPLOY-STAND



- **When to use**: if you require (or prefer) VPN services to be deployed on its own dedicated security appliance. This is used if there will be a high number of VPN connections.
- **Prerequisites**: SEC-NET-VPN, Vendor (Standalone)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: VPN appliance
- **Description**: in this POD, VPN services would be enabled on a dedicated firewall appliance. The VPN appliance would be deployed in-line between the Internet and the DC/LAN as shown in the picture above.

Integrated Deployment

POD: SEC-NET-VPN-DEPLOY-INTG



- **When to use**: if you require (1) using the Internet edge router for VPN services without using a firewall appliance. This is used if there will be a low number of VPN connections (up to 10). Or (2) to support advanced VPN technologies such as DMVPN and GET VPN.
- **Prerequisites**: INET, SEC-NET-VPN, Vendor (Integrated)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Edge router (or WAN router)
- **Description**: in this POD, VPN services would be applied on the Internet edge router (or WAN router) as shown in the picture above.

2.6.3.3 Site-to-Site VPN

Select one of the following VPN technologies that will be used for the Site-to-Site VPN solution:

	IPsec VPN	**DMVPN**	**GET VPN**
	Flex VPN		

IPsec VPN

POD: SEC-NET-VPN-IPSEC1

- **When to use**: if you require building a secure tunnel between two locations over the Internet (or WAN). Or building a secure tunnel between two VPN appliances using different vendor hardware models.
- **Prerequisites**: SEC-NET-VPN-SVPN
- **Required**: SEC2-VPN-IPSEC, Hardware (Router/Firewall)
- **Has Sub-PODs**: --

DMVPN

POD: SEC-NET-VPN-DMVPN

- **When to use**: if you require building secure tunnels between multiple locations over the Internet (or WAN) using Cisco router hardware
- **Prerequisites**: SEC-NET-VPN-SVPN
- **Required**: SEC2-VPN-DMVPN, Hardware (Cisco router)
- **Has Sub-PODs**: --

GET VPN

POD: SEC-NET-VPN-GETVPN

- **When to use**: if you require building secure tunnels between multiple locations over the Internet (or WAN) without using actual VPN tunnels. And will use Cisco router hardware for the network devices.
- **Prerequisites**: SEC-NET-VPN-SVPN
- **Required**: SEC2-VPN-GETVPN, Hardware (Cisco router)
- **Has Sub-PODs**: --

Flex VPN

POD: SEC-NET-VPN-FLEX

- **When to use**: this is an alternative to DMVPN that can support IKEv2
- **Prerequisites**: SEC-NET-VPN-SVPN
- **Required**: Hardware (Cisco router)
- **Has Sub-PODs**: --

Deployment

Below are required, recommended, and optional configuration when deploying Site-to-Site VPN on the network:

Required

- **Encryption**: determine what encryption protocol should be used for the VPN tunnel. Encryption provides confidentiality for IP packets. It is the process where a key (cipher) is used to encrypt and decrypt an IP packet across a VPN connection. The most popular encryption protocols used include AES and 3DES.
- **Authentication**: determine what authentication protocol should be used for the VPN tunnel. Authentication is used to verify the integrity (and its origin) of an IP packet using a one-way hash. The most popular authentication protocols used include SHA-1 and SHA-2. MD5 is a legacy authentication protocol.
- **Key Management**: this is used with all VPN protocols for key management between the VPN nodes. The available options include using a pre-share key or using Certificates.
- **VPN Traffic**: determine what subnets need to communicate with other subnets across the VPN. This is configured in an Access Control List (ACL) for all sites accordingly. Any subnet not listed in the ACL will not be routed over the VPN tunnel.
- **Network Address Translation (NAT):** it is important to disable NAT for the subnets that will be used over the VPN tunnel. Otherwise, the VPN device will try to translate all communication between the sites.

Recommended

- **Encryption using AES**: it is recommended to use AES for the encryption protocol. There are different cipher algorithms that include 128-bit keys (AES-128), 192-bit keys (AES-192), or 256-bit keys (AES-256) for encrypting IP packets. 3DES should only be used if AES is not supported on the VPN device.
- **Authentication using SHA-2**: it is recommended to use SHA-2 for the authentication protocol which provides a higher hash operation. There are different SHA-2 standards available that include 256-bit, 384-bit, and 512-bit. SHA-256 is commonly used if it supported.
- **Key Management using Certificates**: it is recommended to use certificates between sites as a best practice especially if there will be hundreds of VPN devices. Using certificates is more secure and easier to manage, but it requires additional configuration that can be complex from a support perspective. An alternative would be to use pre-shared keys if you have a small number of VPN sites.
- **Key Management using Pre-Share**: this is the most common key management method used and the easiest to setup, but not for managing hundreds of VPN sites. It is also important to note that using pre-shared keys are typically flagged in security audits. Therefore, it is recommended to use a complex pre-share key that changes regularly. Including locking down the VPN nodes with firewall policies based on its WAN facing IP address.

2.6.3.4 Client VPN

Select one of the following VPN technologies that will be used for the client VPN solution:

🟩	**SSL VPN**	**L2TP over IPsec VPN**	**IPsec VPN**

SSL VPN

POD: SEC-NET-VPN-SSL

- **When to use**: if you require users to connect to the corporate network remotely using HTTPS/SSL
- **Prerequisites**: SEC-NET-VPN-CVPN
- **Required**: SEC2-VPN-SSL, Hardware (Router/Firewall supporting SSL VPN)
- **Has Sub-PODs**: --

L2TP over IPsec VPN

POD: SEC-NET-VPN-IPSEC2-L2TP

- **When to use**: if you require users to connect to the corporate network remotely using a native VPN client without using a VPN client program installed on their system
- **Prerequisites**: SEC-NET-VPN-CVPN
- **Required**: SEC2-VPN-IPSEC-L2TP, Hardware (Router/Firewall supporting L2TP over IPsec)
- **Has Sub-PODs**: --

IPsec VPN

POD: SEC-NET-VPN-IPSEC2

- **When to use**: if you require users to connect to the corporate network remotely using a VPN client program installed on their system
- **Prerequisites**: SEC-NET-VPN-CVPN
- **Required**: SEC2-VPN-IPSEC, Hardware (Router/Firewall supporting IPsec for client VPN)
- **Has Sub-PODs**: --

Configuration

Below are required, recommended, and optional configuration when deploying Client VPN on the network:

Required

- **Encryption**: determine what encryption protocol should be used for the VPN tunnel. Encryption provides confidentiality for IP packets. It is the process where a key (cipher) is used to encrypt and decrypt an IP packet across a VPN connection. The most popular encryption protocols used include AES and 3DES.
- **Authentication**: determine what authentication protocol should be used for the VPN tunnel. Authentication is used to verify the integrity (and its origin) of an IP packet using a one-way hash. The most popular authentication protocols used include SHA-1 and SHA-2. MD5 is a legacy authentication protocol.
- **Key Management**: this is used with all VPN protocols for key management between the VPN nodes. The available options include using a pre-share key or using Certificates.
- **IP Address Pool**: determine what dedicated subnet (or range of IP addresses) will be assigned to the VPN clients once they are connected successfully into the network.
- **Network Address Translation (NAT):** it is important to disable NAT for the subnets that will be used over the VPN tunnel. Otherwise, the VPN device will try to translate all communication between the site and the client.

Recommended

- **Encryption using AES**: it is recommended to use AES for the encryption protocol. There are different cipher algorithms that include 128-bit keys (AES-128), 192-bit keys (AES-192), or 256-bit keys (AES-256) for encrypting IP packets. 3DES should only be used if AES is not supported on the VPN device.
- **Authentication using SHA-2**: it is recommended to use SHA-2 for the authentication protocol which provides a higher hash operation. There are different SHA-2 standards available that include 256-bit, 384-bit, and 512-bit. SHA-256 is commonly used if it supported.
- **Key Management using Certificates**: it is recommended to use certificates for the VPN clients if there will be a high number of users. Using certificates is more secure and easier to manage, but it requires additional configuration that can be complex from a support perspective. An alternative would be to use pre-shared keys if you have a small number of VPN clients.
- **Key Management using Pre-Share**: this is the most common key management method used and the easiest to setup. It is also important to note that using pre-shared keys are typically flagged in security audits. Therefore, it is recommended to either use a complex pre-share key that is changed regularly. Or implementing SSL VPN instead which is recommended between the two.
- **Split Tunnel**: this is a recommended feature to specify what traffic should be routed over the secure tunnel for the VPN client. For example, if the VPN clients want to access internal network resources they would be routed over the VPN tunnel. For all other access (e.g. Internet access), they would be routed over their Internet connection.

2.6.4 Identity Control

Select one (or more) of the following identity control PODs that will be used in the solution:

	Identity Control on Firewall	**Identity Control on LAN**	

Identity Control on Firewall
POD: SEC-NET-ID-FW
• **When to use**: if you require filtering traffic based on the user group when accessing the Internet • **Prerequisites**: SEC-NET-FW, SEC-NET-ID • **Required**: -- • **Has Sub-PODs**: Go to 2.6.4.1

Identity Control on LAN
POD: SEC-NET-ID-LAN
• **When to use**: if you require applying security policies directly on the switch ports on the LAN based on the user/group • **Prerequisites**: LAN, SEC-NET-ID • **Required**: -- • **Has Sub-PODs**: Go to 2.6.4.2

2.6.4.1 Identity Control on Firewall

Vendor Solutions

Select one of the following vendors that will be used for identity control on the firewall:

Combined	**Palo Alto Networks** If you require enabling identity control on the Palo Alto Networks firewall appliance along with other security features enabled (e.g. VPN, IPS)	**Fortinet – FortiGate** If you require enabling identity control on the FortiGate firewall appliance along with other security features enabled (e.g. VPN, IPS)
	Cisco – ASA FirePOWER If you require enabling identity control on the Cisco ASA Firepower firewall appliance along with other security features enabled (e.g. VPN, IPS)	**Check Point – Enterprise, SMB** If you require enabling User Awareness on the Check Point firewall appliance along with other security features enabled (e.g. VPN, IPS)

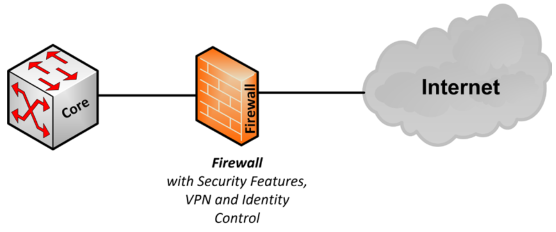
Deployment

Select one of the following deployments that will be used for identity control on the firewall:

🟩	**Combined Deployment**	

Combined Deployment

POD: SEC-NET-ID-FW-DEPLOY-COMB



- **When to use**: if you require identity control services to be enabled on the firewall appliance along with other security features enabled such as VPN, URL, and IPS.
- **Prerequisites**: SEC-NET-FW, SEC-NET-ID-FW
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Firewall appliance
- **Description**: in this POD, identity control services are enabled on the existing firewall appliance as shown in the picture above.

Configuration

Below are required, recommended, and optional configuration when deploying identity control on the firewall appliance:

Required	• **Authentication Mode**: determine how users will be authenticated before accessing services on the Internet. The available options include Active Authentication and Passive Authentication.
Recommended	• **Using Active Authentication**: recommended for guest users, contractors, or any user system not added to Active Directory. The user would be redirected to a web-page (captive portal) to authenticate before gaining access to network resources based on the user group. • **Using Passive Authentication**: recommended for corporate user's that have computers added to Active Directory. This allows the user to login with their AD account and will be able to access Internet services based on the group they are associated to. They are not required to authenticate through a captive portal.
Optional	• None Available

2.6.4.2 Identity Control on LAN

Vendor Solutions

Select one of the following vendors that will be used for Identity control on the LAN.

Standalone	**Cisco – Identity Services Engine (ISE)** If you require identity control for a maximum of 250,000 endpoints using a Cisco enterprise solution	**Fortinet – FortiAuthenticator** If you require identity control between 500 and 100,000 users using a Fortinet enterprise solution
	Microsoft – Network Policy Server (NPS) If you require identity control using the existing on-site Microsoft Active Directory infrastructure	

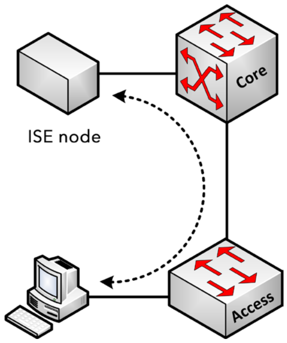
Deployment

Select one of the following deployments that will be used for identity control on the LAN:

	Small Deployment	**Small Deployment with Redundancy**	**Medium Deployment**
	Large Deployment		

Small Deployment

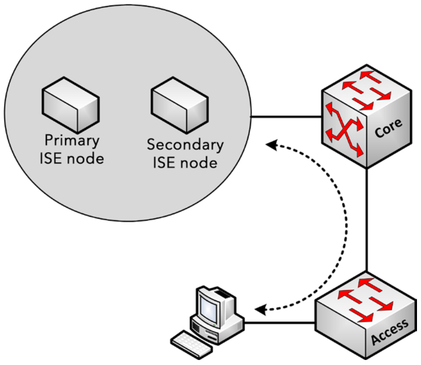
POD: SEC-NET-ID-LAN-ISE-SM1



- **When to use**: if you require identity control up to 20,000 endpoints without high-availability with low traffic usage
- **Prerequisites**: SEC-NET-ID-LAN, Vendor (Cisco ISE)
- **Required**: OPS-AUTH, OPS-SNMP, SEC2-8021X, CDP/LLDP
- **Has Sub-PODs**: --
- **Components**: ISE appliance
- **Description**: in this POD, a single ISE appliance is connected to either the Core switch (or within the server farm) as shown in the picture above. Based on the ISE hardware that is used, a single ISE appliance can support a maximum of 20,000 endpoints.

Small Deployment with Redundancy

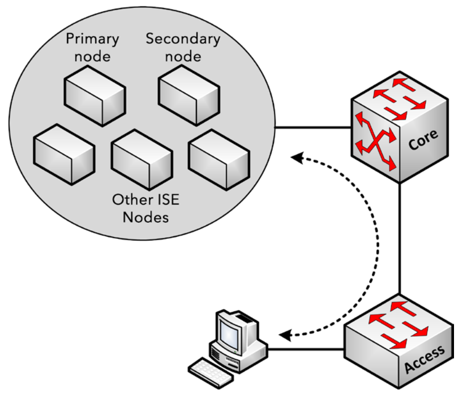
POD: SEC-NET-ID-LAN-ISE-SM2



- **When to use**: if you require identity control up to 20,000 endpoints with high-availability with low traffic usage
- **Prerequisites**: SEC-NET-ID-LAN, Vendor (Cisco ISE)
- **Required**: OPS-AUTH, OPS-SNMP, SEC2-8021X, CDP/LLDP
- **Has Sub-PODs**: --
- **Components**: ISE appliances
- **Description**: in this POD, two ISE appliances are deployed and connected to either the Core switch (or within the server farm) as shown in the picture above. The primary node provides all of the configuration, authentication, and policy capabilities. The secondary Cisco ISE node operates in a backup role.

Medium Deployment

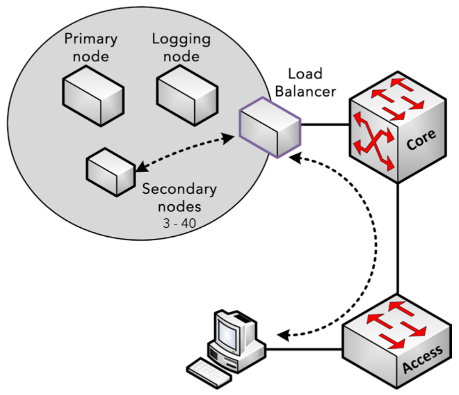
POD: SEC-NET-ID-LAN-ISE-M



- **When to use**: if you require identity control up to 20,000 endpoints with high-availability with moderate traffic usage
- **Prerequisites**: SEC-NET-ID-LAN, Vendor (Cisco ISE)
- **Required**: OPS-AUTH, OPS-SNMP, SEC2-8021X, CDP/LLDP
- **Has Sub-PODs**: --
- **Components**: ISE appliances
- **Description**: in this POD, there are five ISE appliances connected to either the Core switch (or within the server farm) as shown in the picture above. Two of the appliances will be primary and secondary ISE nodes configured for the administration and monitoring personas. The other three ISE appliances will provide network access, posture, guest access, client provisioning, and profiling services.

Large Deployment

POD: SEC-NET-ID-LAN-ISE-L



- **When to use**: if you require identity control up to 500,000 endpoints with high-availability with high traffic usage
- **Prerequisites**: SEC-NET-ID-LAN, Vendor (Cisco ISE)
- **Required**: LB-LOCAL, OPS-AUTH, OPS-SNMP, SEC2-8021X, CDP/LLDP
- **Has Sub-PODs**: --
- **Components**: ISE appliances
- **Description**: in this POD, there can be up to 40 ISE appliances based on the number of endpoints supported for identity control. They will likely be connected to the Core switch as shown in the picture above. There will be a single primary ISE server, a logging server, and several secondary ISE servers behind a load-balancer to optimize the routing of AAA requests to the next available server. All of the network devices would only require a single entry for the AAA servers pointing to a virtual address defined on the load balancing device.

Configuration – Cisco Identity Services Engine (ISE)

Below are required, recommended, and optional configuration when deploying identity control on the LAN using Cisco ISE:

Required

- **Identity Services**: determine how users (or endpoints) will be authenticated on the LAN. The available options include MAB, Profiling, Passive Authentication (802.1x), and Active Authentication (Web Authentication).

Recommended

- **Identity Services using 802.1X**: if you require a user or endpoint to be authenticated using a user account (local accounts or from Active Directory domain). This option requires 802.1X to be enabled on the endpoint and the switch port configured for port authentication. The ISE appliance also needs to be integrated with Active Directory or LDAP for user authentication. This is also called Passive Authentication.
- **Identity Services using Web Authentication**: this is recommended for guest users or endpoints not enabled for 802.1X or its MAC address not added to the ISE appliance. The user would be redirected to a web portal to authenticate before gaining access to network resources. In a Cisco solution, these guest accounts would be managed through a sponsor-based web portal.

Optional

- **Identity Services using MAC Address Bypass (MAB):** if you want the endpoint to be authenticated using only its MAC address and not be prompted to authenticate using a user account. This is common for servers or other network devices you don’t want to be authenticated using an account. This option involves adding the MAC address of the endpoint on the ISE appliance in order for the endpoint to bypass authentication.
- **Identity Services using Profiling**: if you want the endpoint to be discovered for the type of device it is (e.g. Phone, Access List) and apply a specific security policy to its switch port. This is common for implementing identity services with IP Phones or Access Points connected to the network. This option involves setting up device profiles that will allow the ISE appliance to pull information from the LAN switches to determine if the endpoint is an IP phone, an access point, or maybe a Windows/Apple desktop system.

2.6.5 Encryption

Select one (or more) of the following encryption PODs that will be used in the solution:

	MACsec / 802.1AE	**Virtual Private Network (VPN)**	

MACsec / 802.1AE	Virtual Private Network (VPN)
POD: SEC-NET-ENC-MACS	**POD**: SEC-NET-VPN
• **When to use**: if you require encrypting traffic between endpoints locally on the LAN and/or DC. This is typical for high security requirements found in government to financial environments • **Prerequisites**: SEC-NET-ENC • **Required**: LAN/DC • **Has Sub-PODs**: --	• **When to use**: if you require encrypting traffic between sites over an unsecure network (e.g. Internet) • **Prerequisites**: SEC-NET-ENC • **Required**: -- • **Has Sub-PODs**: Go to 2.6.3

2.6.6 Advanced Threat Protection

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for advanced threat protection on the network:

Combined (Cloud)	**Palo Alto Networks - NGFW** If you require deploying advanced threat protection using a cloud-based sandbox, Wildfire, on the existing Palo Alto Networks firewall appliance in the environment	**Fortinet – FortiGate** If you require deploying advanced threat protection using a cloud-based sandbox, FortiSandbox Cloud, on the existing FortiGate firewall appliance in the environment
	Cisco – ASA FirePOWER If you require deploying advanced threat protection using a cloud-based sandbox, Advanced Malware Protection (AMP), on the existing Cisco ASA Firepower firewall appliance in the environment	

Standalone (On-Site)	**Fortinet - FortiSandbox** If you require deploying advanced threat protection using an on-site sandbox due to privacy and regulatory requirements. The private sandbox, using a standalone FortiSandbox appliance, would work with the existing Fortinet security products (e.g. FortiGate, FortiClient, FortiWeb).	**Palo Alto Networks - Wildfire** If you require deploying advanced threat protection using an on-site sandbox due to privacy and regulatory requirements. The private sandbox, using a standalone Wildfire appliance, would work with the existing Palo Alto Networks security products (e.g. NGFW).
	Cisco – NGIPS (AMP) If you require deploying advanced threat protection using an on-site sandbox due to privacy and regulatory requirements. The private sandbox, using a standalone Cisco NGIPS appliance, would work with many of the existing Cisco security products (e.g. ASA Firepower, AMP of Endpoints).	

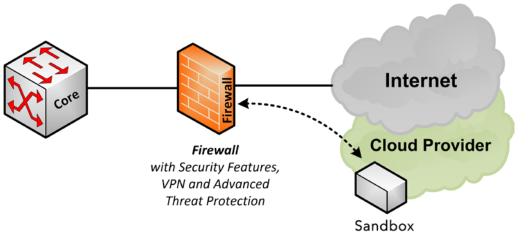
Deployment

Select one of the following PODs for how advanced threat protection will be deployed:

	Combined Deployment	**Standalone Deployment**	

Combined Deployment

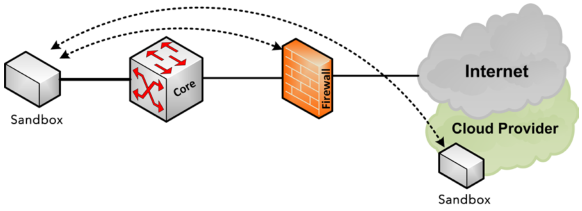
POD: SEC-NET-ATP-COMB



- **When to use**: if you require enabling advanced threat protection on the existing firewall appliance using a cloud-based sandbox
- **Prerequisites**: SEC-NET-ATP, Vendor (Combined)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Firewall, Sandbox
- **Description**: in this POD, advanced threat protection is enabled on the existing firewall appliance and will use a cloud-based sandbox to perform deeper inspection of known and zero day (real time) threats.

Standalone Deployment

POD: SEC-NET-ATP-STD



- **When to use**: if you require enabling advanced threat protection on a standalone sandbox due to privacy and regulatory requirements
- **Prerequisites**: SEC-NET-ATP, Vendor (Standalone)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Firewall, Sandbox
- **Description**: in this POD, the sandbox appliance is connected to the Core switch and would be integrated with its supported firewall appliance to perform deeper inspection of known and zero day (real time) threats.

2.6.7 Web Security

Below are recommended options for securing web servers on the network:

Security Best Practices	**Web Application Firewall (WAF)** If you require a standalone hardware (or software) solution to provide additional application security and protection for the web server farm. Go to 2.6.7.1	**Firewall Restriction** It is recommended to setup firewall policies to restrict who can access the web server from the outside and the internal network

2.6.7.1 Web Application Firewall

Complete each of the design sections below for the solution:

Vendor Solutions

Select one of the following vendors that will be used for the Web Application Firewall (WAF):

Hardware / Software	**Fortinet - FortiWeb** If you require a hardware-based WAF solution using Fortinet hardware providing PCI DSS compliancy. It can provide server load balancing, SSL termination, and vulnerability scanning (e.g. DoS attacks, bots, and other malicious activity). FortiWeb has an extension to support advanced threat protection (level 2 security).	**Sucuri Security - WAF** If you require a software-based WAF to work with web servers running WordPress in the environment. It can also provide malware scanning and server hardening.

2.6.8 Mail Security

Below are recommended options for securing mail servers on the network:

Security Best Practices	**Anti-Spam** To provide email inspection of messages to determine if the message is clean (normal) or a potential spam message	**Anti-Virus** To provide email content inspection of messages for any virus content (e.g. ransomware) embedded that can compromise the desktop endpoint and spread internally
	Email Encryption If you require email messages to be encrypted and sent securely over an unsecure network (e.g. Internet) to a specific recipient who can open the encrypted message	**Firewall Restriction** It is recommended to configure firewall policies on the firewall appliance allowing only SMTP from the email security appliance or from the internal mail server depending on the outbound mail flow. This can prevent users or other servers sending spam/virus enabled messages directly from the network causing congestion and potentially black-listing your mail servers.
	Email Security Appliance If you require a standalone hardware/software solution to provide additional mail security services. Go to 2.6.8.1	

2.6.8.1 Email Security Appliance

Complete each of the design sections below for the solution:

Vendor Solutions

Select one of the following vendors that will be used for the email security appliance:

Hardware	**Cisco – Email Security Appliance** If you require a hardware-based solution to provide anti-spam filtering services. It has an extension to support advanced threat protection (level 2 security) to provide deeper inspection for known and zero day (real-time) threats such as malware found in mail messages.	**Fortinet – FortiMail** If you require a hardware-based solution to provide anti-spam, phishing, file inspection, encryption, to message archiving. It has an extension to support advanced threat protection (level 2 security) to provide deeper inspection for known and zero day (real-time) threats such as malware found in mail messages.

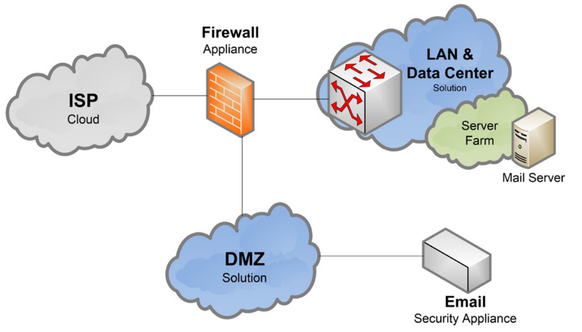
Deployment

Select one of the following email security deployments that will be used in the solution:

🟩	**Out-of-Band (DMZ) Deployment**	**Out-of-Band (SF) Deployment**	**In-Line Deployment**

Out-of-Band (DMZ) Deployment

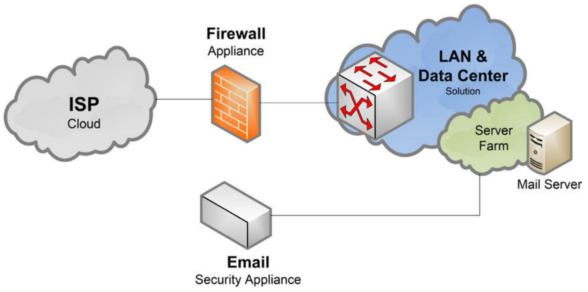
POD: SEC-APP-MAIL-SOL-OOB1



- **When to use**: if you have moderate email traffic and/or require placing the email security appliance in the DMZ
- **Prerequisites**: SEC-NET-MAIL-SOL, INET-DMZ
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Email security appliance
- **Description**: in this POD, the email security appliance is plugged into the DMZ which is connected to the firewall appliance as shown in the picture above.

Out-of-Band (SF) Deployment

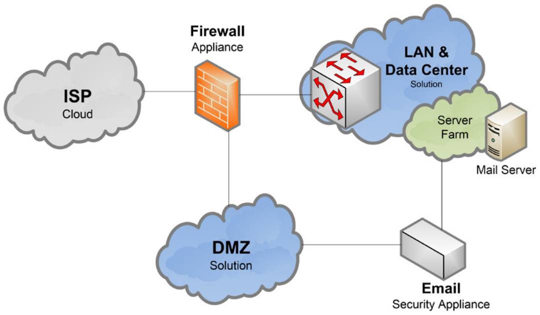
POD: SEC-APP-MAIL-SOL-OOB2



- **When to use**: if you have moderate email traffic and/or require placing the email security appliance in the server farm
- **Prerequisites**: SEC-NET-MAIL-SOL
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Email security appliance
- **Description**: in this POD, the email security appliance is plugged into the Server Farm that exist on the LAN or Data Center as shown in the picture above.

In-Line Deployment

POD: SEC-APP-MAIL-SOL-IL



- **When to use**: if you have heavy email traffic and require placing the email security appliance in-line between the Internet and the Server Farm where the mail server(s) exist. This is the most common and easiest to deploy.
- **Prerequisites**: SEC-NET-MAIL-SOL, INET-DMZ
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Email security appliance (ESA)
- **Description**: in this POD, the external facing interface on the email security appliance deals with mail transfer and filtering to/from the Internet. The internal facing interface deals with transferring mail messages with the internal mail server. This option typically happens when the external facing interface of the ESA connects into the DMZ and the internal facing interface connects directly into the server farm as shown in the picture above.

2.6.9 Remote Desktop Security

Below are recommended options for securing Remote Desktop (or RDP, RDS) on the network:

Security Best Practices	**Firewall Restriction** It is recommended to setup firewall policies to restrict who can RDP into the network	**Strong Password** It is recommended to use strong passwords for any AD account that will RDP into a desktop/server
	User Limitation / Access Limit who can login using RDP with local security policies	**Account Lockout Policy** It is recommended to setup an account lockout policy to protect against brute-force attacks
	Changing RDP Port Another RDP security option would be to change the default RDP port number to some obscure port number for RDP services	**RDP Gateway** This provides the best and recommended option for RDP security. In this solution, the RDP gateway listens for RDP requests over HTTPS and will connect the client to the RDP server on the targeted machine
	Two-Factor Authentication It is recommended to enable two-authentication for highly-sensitive systems to protect against brute-force attacks	**RDP over VPN or SSH** Another RDP security option can involve blocking RDP access into the network from the outside. Instead, the users would connect using a VPN (or SSH) solution. Then build a RDP session over the secure tunnel.

2.6.10 DNS Security

Below are recommended options for securing DNS on the network:

Security Best Practices	**DNS Sinkhole / DNS Filtering** A security feature that can be enabled on a next-generation firewall (if supported) to send a fake DNS response to a user trying to access a high risk (or poor reputation) website. This feature can provide an additional layer of protection against threats if you don't want to implement web filtering services.	**Firewall Restriction** It is recommended to setup firewall policies to restrict what DNS servers can be queried out of the network. It is recommended to block DNS on TCP port 53 if zone transfers between authoritative name servers is not required. Opening DNS on TCP/43 can allow hackers to perform reconnaissance attacks to learn about the network environment to do further damage.

2.6.11 Endpoint Security

Below are recommended options for securing user and server endpoints on the network:

Security Best Practices	**System Updates** It is recommended that the server and user endpoints are regularly updated with OS patches and other software updates	**Anti-Virus** It is recommended to install and maintain an Anti-Virus program on all endpoints with regular scans and real-time inspection (e.g. Web Root)
	Permissions It is recommended to setup permissions for different levels of access to systems on the network including access to files and applications	**User Access Control** It is recommended to enforce User Access control (UAC) capabilities which are based on permissions to ensure that users are not able to install unapproved applications
	Disk Encryption For highly-sensitive systems that have personal information such as client account details, its recommended for those systems to be enabled for disk encryption	**Backup** It is strongly recommended to perform regular backups of critical systems and files on the network in the event of a failure
	Security Agent To achieve a higher level of security for the user endpoints on the network, it is recommended to install security agents. You can enforce security policies for what applications and web-sites users can access on the Internet. Or provide application whitelisting. Go to 2.6.11.1	**RAID** The server endpoint's hard disks can be setup (if supported) in a RAID. RAID has many different types, but RAID5 is the most common which provides drive redundancy where if one drive fails the data is still in-tact and active on another installed drive.

2.6.11.1 Security Agent

Complete each of the design sections below for the solution:

Vendor Solutions

Select one of the following vendors that will be used for the security agent on the endpoints:

Vendor Solutions	**Palo Alto Networks – Traps** If you require using a security agent to integrate with the existing Palo Alto Networks firewall appliance. The agent has an extension to support advanced threat protection (level 2 security) to provide deeper inspection for known and zero day (real-time) threats such as malware.	**Fortinet – FortiClient** If you require using a security agent on to integrate with the existing FortiGate firewall appliance. The agent provides Anti-Virus, URL filtering, application filtering, to vulnerability scanning. The agent has an extension to support advanced threat protection (level 2 security) to provide deeper inspection for known and zero day (real-time) threats such as malware.
	Cisco – AMP for Endpoints If you require using a security agent to integrate with the existing Cisco ASA Firepower firewall appliance. The agent has an extension to support advanced threat protection (level 2 security) to provide deeper inspection for known and zero day (real-time) threats such as malware.	**Carbon Black – CB Protect** If you require whitelisting applications that can be installed on user endpoints to provide stronger protection against ransomware.
	Cisco – Umbrella If you require using a cloud-based security agent to provide URL filtering, reporting, to advanced threat protection for known and zero day (real-time) threats such as malware.	

2.6.12 Cloud Security

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for cloud security:

Vendor Solutions	**Palo Alto Networks - Aperture** If you require visibility and security control for SaaS applications used in the environment. This cloud-based offering provides on-demand scanning of data to detect threats. It can provide reports for audit, compliancy, to user activity with SaaS applications. Aperture has an extension to support advanced threat protection (level 2 security) to provide deeper inspection for known and zero day (real-time) threats such as malware.	**Fortinet – FortiCASB** If you require visibility and security control for SaaS applications used in the environment. This cloud-based offering provides on-demand scanning of data to detect threats. It can provide reports for audit, compliancy, to user activity with SaaS applications.
	Cisco – Cloudlock If you require visibility and security control for SaaS and PaaS used in the environment. This cloud-based offering provides on-demand scanning of data to detect threats such as malware. It can provide reports for audit, compliancy, to user activity with SaaS applications.	

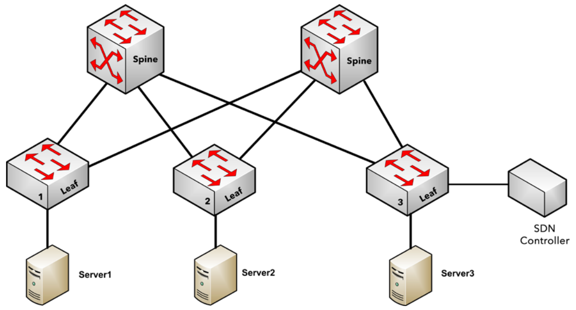
2.7 Software Defined Networks

Select one (or more) of the following Software Defined Network PODs that will be used in the design:

	SDN – Data Center	**SD-WAN - WAN**

Data Center (SDN)

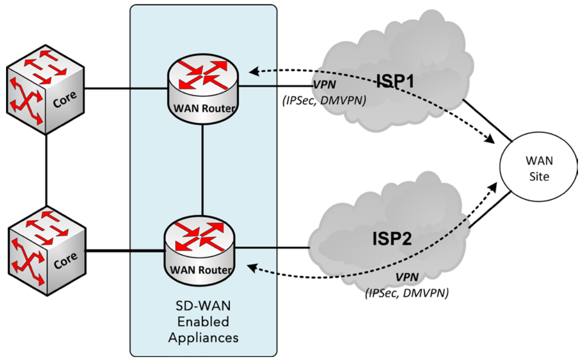
POD: SDN-DC



- **When to use**: if there is a lot of machine-to-machine communication with similar functions and you want to manage the entire network from a centralized controller
- **Prerequisites**: DC-CLOS
- **Required**: --
- **Has Sub-PODs**: Go to 2.7.1
- **Components**: Spine switch, Leaf Switch, SDN controller
- **Description**: this POD will consist of one (or more) leaf switches connecting to one (or more) spine switches. The server endpoints would be connected to the Leaf switches. The topology will also consist of a SDN controller appliance connected to one (or more) of the Leaf switches.

WAN (SD-WAN)

POD: SDN-WAN



- **When to use**: if you require optimizing application traffic (based on performance and latency) between sites using low-cost connectivity options (e.g. Internet).
- **Prerequisites**: WAN
- **Required**: --
- **Has Sub-PODs**: Go to 2.7.2
- **Components**: SD-WAN Appliance (or WAN router)
- **Description**: in this topology, a SD-WAN enabled device would be connected to one or more service providers as shown in the picture above. The appliance will connect down into to either the Core switch (LAN/DC) or the Network Services switch in the topology.

2.7.1 Data Center (SDN)

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for the SDN solution:

Hardware based SDN	**Cisco – ACI** If you require building a SDN managed Data Center using Cisco hardware	**Fortinet - FortiCore** If you require building a SDN managed Data Center using Fortinet hardware which also provides support for OpenFlow
	Open Source If you require building a SDN managed Data Center using open-source hardware & software options	**Juniper - Contrail** If you require building a SDN managed Data Center using Juniper hardware

Software based SDN	**Open Source** If you require building a SDN managed Data Center using open-source hardware & software options	**VMware – NSX** If you require building a SDN managed Data Center using VMware software

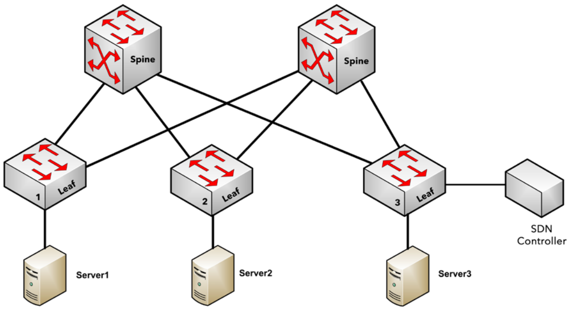
Deployment

Select one of the following SDN deployment(s) that will be used in the solution:

	Hardware Deployment	

Hardware Deployment

POD: SDN-DC-DEPLOY-HW



- **When to use**: if you require building a hardware-based SDN in the Data Center using physical SDN enabled switches
- **Prerequisites**: SDN-DC, Vendor (Hardware-Based SDN)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Spine switch, Leaf Switch, SDN controller
- **Description**: in this POD, there are one (or more) leaf switches connected to one (or more) spine switches as shown in the picture above. The server endpoints would be connected to the Leaf switches. The topology will also consist of a SDN controller appliance connected to one (or more) Leaf switches.

Configuration – Cisco ACI

Below are required, recommended, and optional configuration when deploying SDN using Cisco ACI:

Required

- **Hardware for Spine-Leaf Switches**: the topology requires that the spine and leaf switches consist of Cisco Nexus 9K series hardware
- **Hardware for SDN Controller**: the topology requires using Cisco APIC for the SDN controller.

- **Tenant**: first define a logical container that will hold all routing and switching functions
- **Private Network**: define a private network which will provide the IP address space for the tenant previously added. This would be equivalent to adding a VRF instance.
- **Bridge Domain**: define all bridge domains that will be used which would be a Layer-2 domain that would be associated to a Private network. This would be equivalent to adding a VLAN.
- **Subnet**: define all IP subnet blocks that will be used and associate them to a bridge domain. This would be equivalent to adding a VLAN SVI to an existing VLAN (bridge domain) to make that network routable.
- **Application Profiles**: a necessary component that is used to define what server endpoints can access within the SDN topology.
- **End Point Groups**: one (or more) groups are defined inside of an existing application profile to describe common services and policies that are used within a server farm.
- **Switch Profiles**: add a profile that will be used to group one (or more) leaf switches in the topology.
- **Switch Selector**: specify each Leaf switch in the topology. This would be associated to a switch profile.
- **Interface Profiles**: add a profile that can be used for grouping a range of interfaces on a particular Leaf switch. This interface profile would be associated to a single switch profile.
- **Access Port Selectors**: define a switch port or a range of switch ports on the Leaf switch that may be commonly configured. The access port selectors would be associated to an Interface profile.
- **Interface Policy Groups**: define all groups that will be used to configure a common group of ports or Access Port Selectors. There are three types of Interface policy groups that can be added. There is access port policies, port channel interface policies, and VPC interface policies. An interface policy group would be a mapped to a single Access port Selector.
- **Interface Policies**: this will be policies added to an interface policy group that will specify how a group of ports will be configured. Some of these interfaces policies include: (1) Link level interface policies for 1G and 10G. (2) CDP interface policies to define if CDP should be enabled or disabled. (3) LLDP interface policies to define if LLDP should be enabled or disabled. (4) Port Channel interface policies for LACP to define bundling multiple interfaces together.
- **Attachable Access Entity Profiles (AEP)**: an AEP needs to be defined to map the physical interfaces and the VLANs that will be defined.
- **Domains**: used to store different types of VLANs that can be used with a group of switch ports. A domain can be setup as a physical domain which means a standard Layer-2 broadcast domain (e.g. VLAN). It can be a VMM domain which is used to permit VLANs with a directly attached hypervisor host. You can setup a Layer-2 external domain or a Layer-3 domain if the VLANs will be used externally. This domain would be associated to an AEP and a VLAN pool.
- **VLAN Pools**: add all VLAN IDs that will be used and map them to its correct **Domain**.

Recommended

- Define one Switch Profile (with a single Switch Selector) for each leaf switch in the topology
- Define one Switch Profile for each pair of leaf switches that will be used for VPCs. This switch profile will have two Switch Selectors listing each of the VPC enabled leaf switches.
- Define one Interface Profile for each Switch Profile
- Define one Access Port Selector for each switch port that will be used in a Switch Profile. Do not define a range of switch ports.
- Add a single VLAN ID to a single VLAN Pool. This will provide more flexibility if you need to remove a VLAN from a pool.

Optional

- **Filtering between Server Groups**: if you want to restrict access between different server farms within the SDN topology, you first need to specify the "**Filters**" listing what protocols and ports should be allowed such as TCP/80 and TCP/443. Next, a "**Subject**" needs to be created which will define one (or more) filters. These subjects are like creating an application group. For example, we can add a Subject called "Web" that will list filters for TCP/80 and 443. Lastly, associate the subject(s) to a "**Contract**". This contract would be applied to different end point groups to specify what clients can access within the server farm.
- **VPC Protection Groups**: used to define a pair of switches that will be configured for Virtual Port Channels.

2.7.2 WAN (SD-WAN)

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for the SD-WAN solution:

Vendor Solutions	**Cisco – Intelligent WAN (IWAN)** If you require building a SDN managed WAN using Cisco ASR / ISR hardware	**Cisco – Meraki MX** If you require building a SDN managed WAN using cloud-based Cisco Meraki hardware
	Riverbed If you require building a SDN managed WAN using Riverbed Steelhead-SD hardware	**Silver Peak – Unity EdgeConnect** If you require building a SDN managed WAN using a Silver Peak Unity EdgeConnect hardware solution

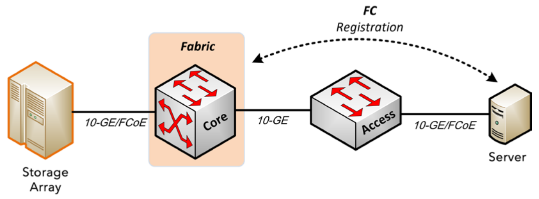
2.8 Storage

Select one (or more) of the following Storage PODs that will be used in the design:

Array & Servers using FCoE	**Array & Servers using Fibre Channel**	**Array & Servers using Single Fibre Channel Switch**
Array Servers using Dual Fibre Channel Switch	**Array using FCoE & Servers using iSCSI**	**Array using Fibre Channel & Servers using FCoE**
Array & Servers using iSCSI		

Array & Servers using FCoE

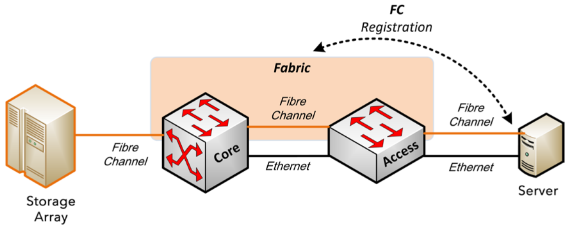
POD: SAN-FCOE



- **When to use**: if you require the storage array and servers to be connected into the existing Data Center switches using FCoE for the storage transport. This POD is typically recommended for a SAN.
- **Prerequisites**: SAN
- **Required**: FCOE
- **Has Sub-PODs**: --
- **Components**: Storage Array, Servers
- **Description**: in this topology, the storage array is connected into the DC core switch using FCOE. The servers (with CNA) would be connected into the DC access (or core switch) using FCoE as shown in the picture above.

Array & Servers using FC

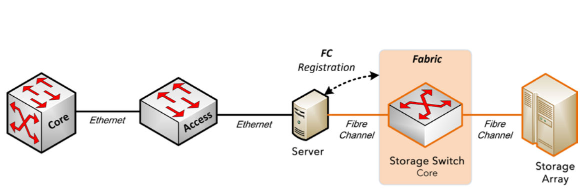
POD: SAN-FC1



- **When to use**: if you require the storage array and servers to be connected into the existing Data Center switches using Fibre Channel for storage transport. This POD is typically not used nor recommended.
- **Prerequisites**: SAN
- **Required**: FC
- **Has Sub-PODs**: --
- **Components**: Storage Array, Servers
- **Description**: in this POD, the storage array is connected into the DC core switch using FC. The servers (with HBA) would also be connected into the DC access (or core switch) using FC as shown in the picture above.

Array & Servers using Single FC Switch

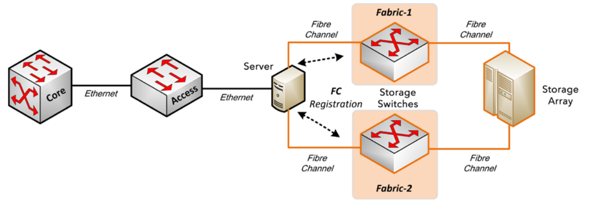
POD: SAN-FC2



- **When to use**: if you require building an isolated storage network using Fibre Channel with no redundancy
- **Prerequisites**: SAN
- **Required**: FC, FC switch
- **Has Sub-PODs**: --
- **Components**: Storage Array, Servers, FC switch
- **Description**: in this POD, the storage array and the servers (with HBA) are connected into a dedicated storage switch using FC as shown in the picture above.

Array & Servers using Dual FC Switch

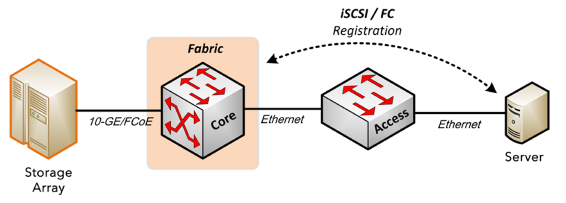
POD: SAN-FC3



- **When to use**: if you require building an isolated storage network using Fibre Channel with high-availability
- **Prerequisites**: SAN
- **Required**: FC, FC switch
- **Has Sub-PODs**: --
- **Components**: Storage Array, Servers, FC switch
- **Description**: in this POD, the storage array and the servers (with HBA) are connected to a pair of redundant (with separate fabrics) storage switches using FC as shown in the picture above.

Array using FCoE & Server using ISCSI

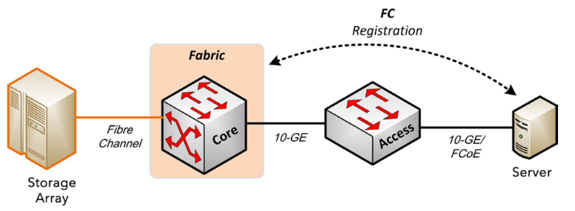
POD: SAN-FCOE-ISCSI



- **When to use**: if you require the storage array to be connected into the existing Data Center switches using FCoE. But the servers will connect into the storage fabric using iSCSI.
- **Prerequisites**: SAN
- **Required**: FCOE, ISCSI
- **Has Sub-PODs**: --
- **Components**: Storage Array, Servers
- **Description**: in this POD, the storage array is connected into the DC core switch using FCOE. The servers would be connected into the DC access (or core switch) and will use ISCSI to register with the storage fabric.

Array using FC & Server using FCoE

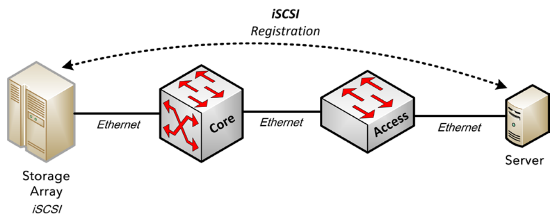
POD: SAN-FC-FCOE



- **When to use**: if you require the storage array to connect into the existing Data Center switches using Fibre Channel, but the servers will use FCOE.
- **Prerequisites**: SAN
- **Required**: FCOE, FC
- **Has Sub-PODs**: --
- **Components**: Storage Array, Servers
- **Description**: in this POD, the storage array would be connected into the DC core switch using Fibre Channel. The servers (with CNA) would be connected into the DC access (or core switch) using FCoE.

Array & Servers using ISCSI

POD: SAN-ISCSI



- **When to use**: if you require the storage array and servers to use ISCSI. This POD is common for small and SMB-sized networks.
- **Prerequisites**: SAN, LAN/DC
- **Required**: OPS-JUMBO, OPS-FC
- **Has Sub-PODs**: --
- **Components**: Storage Array, Servers
- **Description**: in this POD, the storage array and the servers are connected into a dedicated Ethernet switch as shown in the picture above.

Configuration

Below are required, recommended, and optional configuration when deploying a storage solution on the network:

Required

- **Licensing**: to enable the use of Fibre Channel and/or Fibre Channel over Ethernet (FCoE) on Cisco Nexus switches (if applicable) it requires the appropriate license to be activated
- **Virtual SAN (VSAN):** used to build a logical fabric on a single SAN switch (e.g. Cisco MDS 9100). Each VSAN has its own set of services and address space which prevents an issue in one VSAN from affecting other VSANs. Each VSAN is completely isolated which is a strong recommendation.
- **Zoning**: to provide a SAN fabric to restrict visibility and connectivity among devices connected to a SAN. This can be done for controlling which initiators can see which targets. Targets are basically disks or tape devices. Initiators are servers that connect to a disk (or tape) on the storage array. You can configure a single initiator and a single target per zone. Or you can configure a single initiator to multiple targets in the same zone. However, you should limit zoning to a single initiator and target. Initiator-based zoning allows a switch port to be independent by using the world-wide name (WWN) of the server endpoint.

Recommended

- **Device Aliases**: it is recommended to use a user-friendly naming format for pWWNs in a SAN fabric. For example, let’s say we have a device alias for "r1a-c210-srv1-hba0-p1". This means our server named SRV1 (Cisco UCS 210) is located in rack 1A in our data center. This server is plugged into a FC switch port from its primary HBA (hba0) on port 1.
- **Quality of Service (QoS) for FCoE**: recommended to provide lossless data for all FCoE traffic end-to-end across the Data Center.
- **Management using Cisco DCNM**: if you are using Cisco based Data Center hardware with storage components, it is recommended to use the Cisco Data Center Network Manager (DCNM) for SAN essentials for managing the storage configuration (e.g. VSANs, zones, device aliases).

Optional

- **Fibre Channel over IP**: if you require extending Fibre Channel traffic over an L3 WAN. Fibre Channel connections can be extended across long distances (in a WAN solution) using Fibre Channel over IP (FCoIP) on a supported SAN switch (e.g. Cisco MDS 9148).

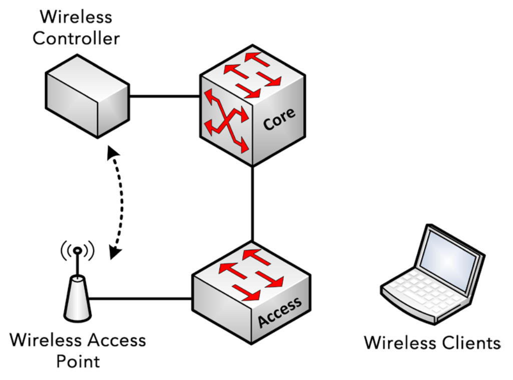
2.9 Wireless

Select one (or more) of the following Wireless PODs that will be used in the design:

	Wireless LAN (WLAN)	

Wireless LAN

POD: WIFI-LAN



- **When to use**: if you require providing wireless access for user endpoints on the LAN
- **Prerequisites**: WIFI, LAN
- **Required**: SW, PWR-POE, OPS-DHCP
- **Has Sub-PODs**: Go to 2.9.1
- **Components**: Wireless Controller, Access Points
- **Description**: in this POD, access points are controlled by a centralized controller which will be connected to the Core switch or Network services switch. The access points would be connected across one (or more) access switches in the topology.

2.9.1 Wireless LAN

Complete each of the design sections below for the solution.

Vendor Solutions

Select one of the following vendors that will be used for the Wireless LAN solution:

On-Premise	**Cisco – Aironet AP & WLC** If you require using an enterprise on-site solution using Cisco Aironet and WLC (standalone) hardware. The WLC appliance would be a standalone appliance in the environment.	**Cisco – Catalyst 3K with WLC** If you require using an enterprise on-site solution using Cisco Aironet and WLC (integrated) hardware. The WLC appliance would be integrated within a supported Cisco Catalyst switch in the environment.

Cloud	**Cisco – Meraki MR** If you require using a cloud-based SMB solution offered by Cisco Meraki. The controller would be managed in the cloud with access points physically connected across the network.	**AeroHive** If you require using a cloud-based SMB solution offered by AeroHive. The controller would be managed in the cloud with access points physically connected across the network.

Hybrid	**Ubiquiti - UniFi** If you require using an enterprise and/or cloud-based SMB solution offered by Ubiquiti. The controller can be deployed in the cloud (for free) or managed locally on-site on a server (or key server). The access points would be physically connected across the network.	

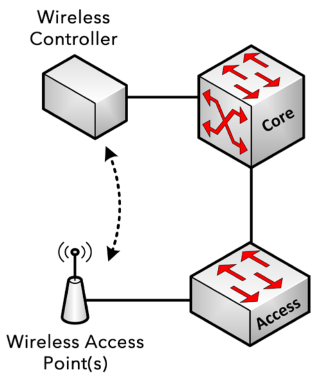
Deployment

Select one of the following wireless deployments that will be used in the solution:

	On-Premise Deployment - Standalone	**On-Premise Deployment - Integration**	**Cloud Deployment**
	On-Premise Deployment - Remote	**Hybrid Deployment**	

On-Premise Deployment - Standalone

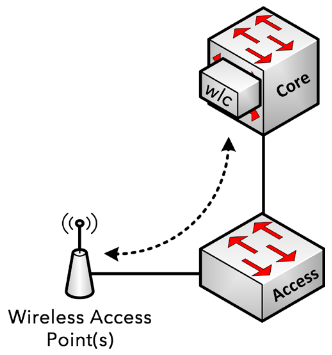
POD: WIFI-LAN-ONSITE-STD



- **When to use**: if you require implementing a standalone controller and access points at a single site that you will manage for all administrative tasks. Or if 100+ access points will be used in the environment.
- **Prerequisites**: WIFI, Vendor (On-Premise - WLC)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Wireless Controller (Local), Access Points
- **Description**: in this POD, the access points are controlled by a centralized controller (local mode) which will be connected to the Core switch or the Network services switch. The access points would be connected across one (or more) access switch on the LAN. This topology is also recommended if the environment will have 100+ access points.

On-Premise Deployment - Integration

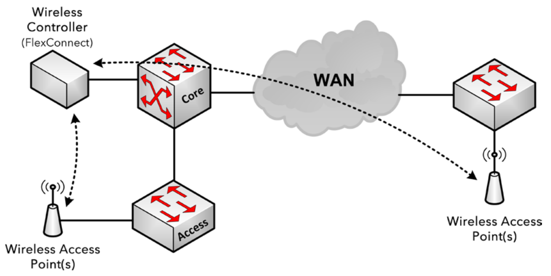
POD: WIFI-LAN-ONSITE-INTG



- **When to use**: if you require implementing an on-site wireless solution where the controller is consolidated within the Core switch in the environment
- **Prerequisites**: WIFI, Vendor (On-Premise – Catalyst 3K with WLC)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Core Switch with Wireless Controller, Access Points
- **Description**: in this POD, the access points are controlled by a centralized controller which is consolidated within the Core switch as shown in the picture above. The access points would be connected across one (or more) access switch on the LAN.

On-Premise Deployment - Remote

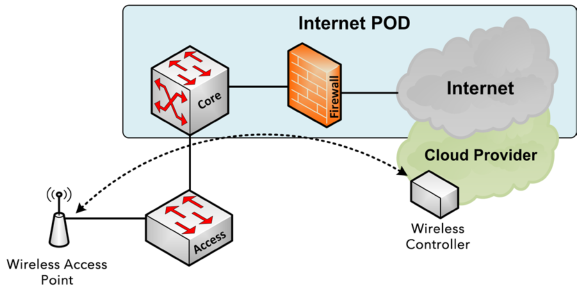
POD: WIFI-LAN-ONSITE-RS



- **When to use**: if you require implementing a single wireless controller with access points located at smaller remote sites on WAN
- **Prerequisites**: WAN, WIFI, Vendor (On-Premise – Cisco WLC)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Wireless Controller (FlexConnect), Access Points
- **Description**: in this POD, multiple small remote-sites with access points are controlled by a centralized controller (FlexConnect mode). The controller would be connected to the Core switch or Network services switch at the main office. Access points would be connected access one (or more) access switches at the main office including remote sites (with latency less than 100ms). FlexConnect supports a mobility group of up to 50 access points.

Cloud Deployment

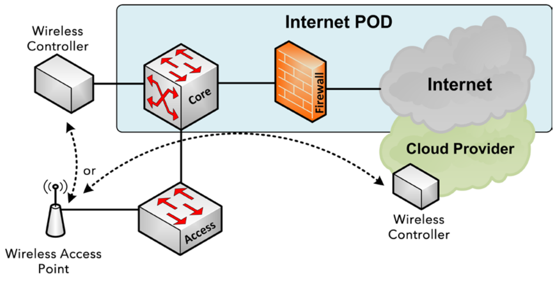
POD: WIFI-LAN-CLD



- **When to use**: if you require using a cloud-based controller that is not on-site, but will have access points connected physically at the site
- **Prerequisites**: INET, WIFI, Vendor (Cloud)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Cloud-based Controller, Access Points
- **Description**: in this POD, the access points are controlled by a centralized controller that is located on the Internet. The access points would be connected across one (or more) access switch on the LAN.

Hybrid Deployment

POD: WIFI-LAN-HYBRID



- **When to use**: if you require implementing a standalone controller and access points on-site that you will manage for all administrative tasks. Plus, support to manage the wireless network from the Internet if needed.
- **Prerequisites**: WIFI, Vendor (Hybrid)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Wireless Controller, Access Points
- **Description**: in this POD, the access points are controlled by an on-site wireless controller connected to the Core switch or Network services switch. The wireless network can also be managed via the Internet (Cloud Dashboard). The access points themselves would be connected across one (or more) access switch on the LAN.

Configuration

Below are required, recommended, and optional configuration when deploying a Wireless LAN solution on the network:

Required

- **Wireless Networks (SSID):** determine what wireless networks (SSIDs) will be configured based on the type of user groups. This can be a wireless network for Corporate users, Guest users, or some other custom use-case. Each wireless network (SSID) should be associated to a VLAN. 802.1Q Trunking is used to support multiple VLANs across the LAN.
- **Wireless Standard**: determine the 802.11 services that should be used for the wireless access points. Current 802.11 bandwidth technologies include 802.11g, 802.11n, and 802.11ac
- **Wireless Security**: determine the security that will be used with the wireless network based on the encryption and authentication method. This includes methods such as WPA, PEAP, and EAP-TLS.
- **Power over Ethernet (PoE) for Access Points**: it is recommended to provide power to the access points from its connected access switch. This can avoid using a power adapter for all access points.
- **DHCP for Access Points**: required for the access points to get an IP address and connect to the wireless controller. If you are using a Cisco Aironet wireless solution, DHCP option 43 is required to map the access points to the WLCs.

Recommended

- **Site Survey**: it is highly recommended to conduct a wireless site survey for access point placement on the network. The site survey should consider the number of potential wireless users and concurrent wireless users in a particular area of the building. It should consider the building layout by referencing the building blueprints to determine the square footage for the area you want the wireless network to cover. It should determine all of the noise and interference components such as other 802.11 devices, building material such as glass, concrete, and metal. Also determine if the wireless coverage will be used inside or extended outside of the building(s).
- **Wireless Network for Corporate Users**: it's recommended to add a wireless network for employees to access internal network resources and the Internet.
- **Wireless Network for Guest Users (BYOD):** it's recommended to add a wireless network to allow access to the Internet. Access to other networks (e.g. internal networks) should be restricted.
- **Wireless Security for Guest Users (BYOD):** it is recommended to enable open authentication for the guest SSID, but also provide a method where connected Guest users access a centralized Guest portal (or captive portal) page before gaining network access. The portal page may require user authentication or accepting a disclaimer defined by a security policy.
- **Wireless Standard using 802.11n/802.11ac**: it is recommended to consider implementing either 802.11n and/or 802.11ac (Wave 2) for the wireless radios. 802.11n can provide data rates up to 300Mb/s per access point by using wider WIFI channels (40 MHz wide channels). And 802.11ac, also called Gigabit WIFI, can provide data rates between 433Mbps to 1.3Gbps by combining two of the 40MHz wide channels to 80MHz. Furthermore, 802.11ac only supports 5GHz (not 2.4GHz).
- **Wireless Encryption using WPA2/AES (802.11i):** it is recommended to deploy WPA2 using AES for wireless encryption for the wireless networks. If this is not supported, an alternative can be WPA using TKIP.
- **Wireless Authentication using PEAP MS-CHAPv2:** this is recommended for wireless authentication for corporate wireless networks. This would force a user to authenticate (against Active Directory using RADIUS) before gaining network access. Certificates are only required on the RADIUS server.

Optional	• **Antennas on Access Points**: determine the type of antennas that will be used to provide wireless coverage in unique areas with interference and building material such as glass or concrete. It can also provide wireless coverage across long distances if the wireless network extends to the outside (or inside). If the site survey and the building has any of these components consider external antennas for the access points in the design. • **Wireless Controller Redundancy**: if supported by the Wireless controller, for redundancy, multiple Wireless Controller appliances can be configured together to provide redundancy for the Access Points. You can also add additional access points to provide continued coverage if (1) one or more access point fails and (2) if an access point gets oversubscribed with connected users. • **Wireless Authentication using EAP-TLS and PEAP MS-CHAPv2**: this is required for achieving the most secure wireless authentication, but it is the most complex to administer. This method uses certificates on the RADIUS server and the wireless clients, plus the users must authenticate before gaining network access. • **VPN across Wireless Solution**: for unique requirements that require connecting the wireless network on the outside of the network. The corporate users would then VPN (using IPsec or SSL VPN) into the network to access internal resources. This does provide an additional layer of security (integrity and confidentiality) for the Wireless network. However, this is typically not common nor recommended. • **Link Aggregation (LAG):** if you need to bundle multiple Ethernet connections between the wireless controller (if supported) and the LAN core switch to achieve higher bandwidth resources. Port Channel would be required on the LAN core switch if LAG will be setup. • **Cisco FlexConnect**: used to locally switch wireless packets at remote sites. This should be used if Lightweight access points are deployed at the remote site connecting to a controller located at the HQ site. If FlexConnect is not enabled for the remote site access points, then traffic could be routed back to the HQ site then to the remote site even for local traffic. Furthermore, with a remote site access point enabled for FlexConnect, if the WAN is down and/or cannot communicate with the Wireless LAN Controller, it will act as a standalone access point. • **Cisco CleanAir**: this is a Cisco wireless tool that is built into an access point. It monitors radio interference acting as a built-in spectrum analyzer to provide self-healing and self-optimization on the wireless network. It doesn't eliminate wireless interference nor pollution in the air, but it allows the access points to dynamically adjust its signal to avoid it. Cisco CleanAir also provides performance protection for 802.11n networks.

3. Services

Select one (or more) of the following services that will be used in the design:

Energy / Power	**IPv6**	**Multicast**
Network Address Translation (NAT)	**Operations**	**Overlay / Tunneling**
Quality of Service (QoS)	**Reliability**	**Routing**
Security	**Switching**	**Virtualization**

Energy / Power

POD: PWR

- **When to use**: if you require energy efficient services and/or require providing power to endpoints such as phones and access points
- **Prerequisites**: LAN
- **Required**: --
- **Has Sub-PODs**: Go to 3.1

IPv6

POD: IPV6

- **When to use**: if you will be enabling IPv6 addressing among your network devices and endpoints
- **Prerequisites**: LAN and/or DC
- **Required**: --
- **Has Sub-PODs**: Go to 3.2

Multicast

POD: MCAST

- **When to use**: if your network will consist of voice, video, and/or multicast-enabled applications to provide efficient data, voice, and video delivery across the network
- **Prerequisites**: LAN and/or DC
- **Required**: --
- **Has Sub-PODs**: Go to 3.3

Network Address Translation (NAT)

POD: NAT

- **When to use**: if you want your internal network using private addressing to access the Internet
- **Prerequisites**: INET
- **Required**: --
- **Has Sub-PODs**: Go to 3.4

Operations

POD: OPS

- **When to use**: user, network, and vendor specific services that can be implemented on the network devices to provide a specific operational function
- **Prerequisites**: LAN and/or DC
- **Required**: --
- **Has Sub-PODs**: Go to 3.5

Overlay / Tunneling

POD: OVR

- **When to use**: if you want to extend VLANs between multiple Data Centers and/or tunneling of traffic between Data Center switches
- **Prerequisites**: DC and/or WAN
- **Required**: --
- **Has Sub-PODs**: Go to 3.6

Quality of Service (QoS)

POD: QOS

- **When to use**: if your network will be implemented for any Collaboration or Video solution. Or if providing application and/or endpoint traffic priority is important
- **Prerequisites**: LAN
- **Required**: --
- **Has Sub-PODs**: Go to 3.7

Reliability

POD: REL

- **When to use**: if you require implementing additional redundancy-based services on the network devices
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 3.8

Routing

POD: RT

- **When to use**: required if your network will consist of 3 or more network devices
- **Prerequisites**: LAN/DC, SW
- **Required**: --
- **Has Sub-PODs**: Go to 3.9

Security

POD: SEC2

- **When to use**: if you require VPN and ACL services to be implemented on the network based on a chosen security solution. Including providing a list of best practices that should be implemented on all network devices.
- **Prerequisites**: SEC-NET-VPN, SEC-NET-FW
- **Required**: --
- **Has Sub-PODs**: Go to 3.10

Switching

POD: SW

- **When to use**: if you require networks to be used by various endpoints across a LAN and/or Data Center
- **Prerequisites**: LAN and/or DC
- **Required**: --
- **Has Sub-PODs**: Go to 3.11

Virtualization

POD: VRT

- **When to use**: if you require creating isolated networks or network functions that can be used for connecting customer networks. This will provide traffic and route separation between the customer networks.
- **Prerequisites**: SP, LAN and/or DC
- **Required**: --
- **Has Sub-PODs**: Go to 3.12

3.1 Energy / Power

Select one (or more) of the following energy/power services that will be used in the design:

	Power over Ethernet (PoE)	**EnergyWise**	**EEE**

Power over Ethernet (PoE)

POD: PWR-POE

- **When to use**: if you require the network switches to provide power to a connected IP Phone, Wireless Access Point, or Virtual Desktop
- **Prerequisites**: IP Phone and/or Access Point
- **Required**: Switches (POE)
- **Has Sub-PODs**: Go to 3.1.1

EnergyWise

POD: PWR-EW

- **When to use**: an optional feature that you can enable on your switches with IP phones by reducing the device's power consumption when network traffic is idle or low.
- **Prerequisites**: --
- **Required**: Cisco Catalyst switches
- **Has Sub-PODs**: --

EEE

POD: PWR-EEE

- **When to use**: an optional feature similar to EnergyWise, that can be enabled on Cisco Small Business switches by reducing the device's power consumption when network traffic is idle or low.
- **Prerequisites**: --
- **Required**: Cisco Small Business switches
- **Has Sub-PODs**: --

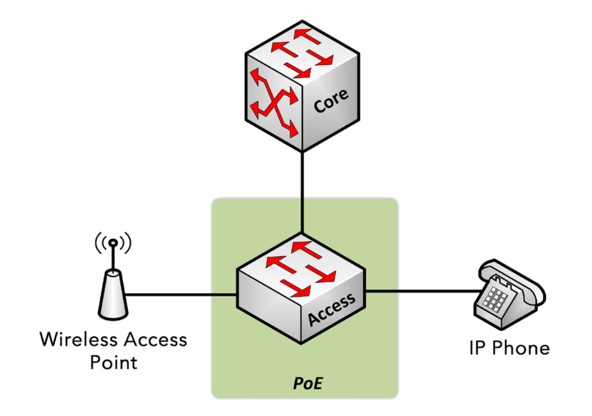
3.1.1 Power over Ethernet

Select one (or more) of the following PoE deployments that will be used:

	Deployment in LAN POD	

Deployment in LAN POD

POD: PWR-POE-LAN



- **When to use**: if you require POE support on the LAN access switches to provide power to the IP phone and access points
- **Prerequisites**: PWR-POE
- **Required**: Switches (POE)
- **Has Sub-PODs**: --
- **Components**: LAN access switch
- **Description**: in this POD, the access switches in the LAN POD will have POE capabilities.

Configuration

Select one (or more) of the following PoE options that will be used:

	PoE Supports up to 15 watts per port. Used for IP phones and legacy wireless access points (e.g. 802.11g)	**PoE+** Supports up to 30 watts per port. Used for enhanced IP phones and wireless access points (e.g. 802.11ac).	**Unified PoE** Supports up to 60 watts per port. Used for virtual desktops over the same cabling utilized by PoE+.

Below are required, recommended, and optional configuration when deploying PoE services on the network based on the available options:

Required	• **PoE Type**: determine what type of PoE is needed based on the devices that will be used. The available options include PoE, PoE+, and Unified PoE. • **Hardware**: the LAN access switch model must support Power over Ethernet (PoE)

Recommended	• **Using PoE+:** it is recommended to consider PoE+ to support more of the enhanced IP phones and gigabit wireless access points (e.g. 802.11ac) that exist today. • **Using Unified PoE**: this is recommended if you will have virtual desktops that can be powered via PoE.

3.2 IPv6

Select one (or more) of the following IPv6 PODs that will be used in the design:

	IPv6 Deployment	**IPv6 Addressing - Network**	**IPv6 Addressing - Interface-ID**

IPv6 Deployment

POD: IPV6-DEPLOY

- **When to use**: this is required for deploying IPv6 services based on existing solutions such as the LAN, WAN, and Internet
- **Prerequisites**: LAN/DC
- **Required**: IPV6-ADD-NET, IPV6-ADD-INTF
- **Has Sub-PODs**: Go to 3.2.1

IPv6 Addressing - Network

POD: IPV6-ADD-NET

- **When to use**: this is required to determine the type of addressing that will be used by the endpoints (and network devices)
- **Prerequisites**: IPV6-DEPLOY
- **Required**: --
- **Has Sub-PODs**: Go to 3.2.2

IPv6 Addressing – Interface-ID

POD: IPV6-ADD-INTF

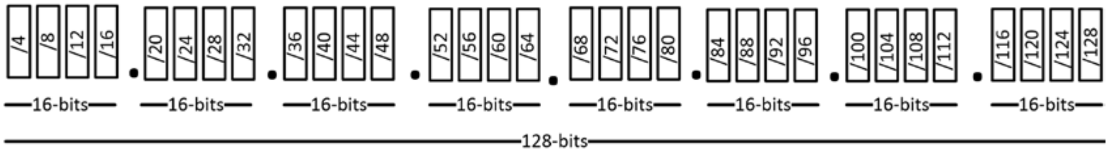
- **When to use**: this is required to determine how the Interface-ID of an IPv6 address will be created on the endpoints
- **Prerequisites**: IPV6-DEPLOY, IPV6-ADD-NET
- **Required**: ATT-STD-ADDR-V6
- **Has Sub-PODs**: Go to 3.2.3

Concepts

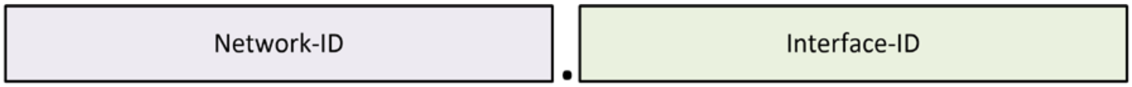
Below is a quick overview of the IPv6 addressing structure:

The total bits within a IPv6 address is 128-bits long consisting of eight 16-bit fields. Within each 16-bit field, it will consist of four sub-fields that is 4-bits long.

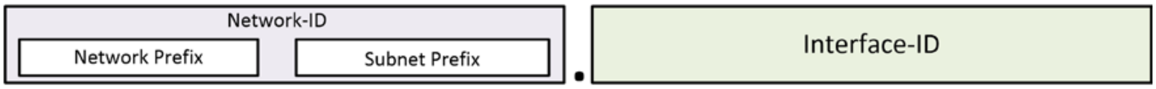
An IPv6 address uses hexadecimal values which ranges from 0 to 9 and A to F. This will provide 16 possible values that can be used for each sub-field in the address.



An IPv6 address is broken up into two main parts: Network-ID + Interface-ID:



The Network-ID is broken down further based on the Network Prefix and the Subnet Prefix:



For example, the Network-ID may be fd00:1::/64. In this network-ID, the network prefix would be "fd00" and the subnet prefix would be "1". Together they will make up the network-ID, similar to IPv4.

The /64 indicates that the first 64-bits are used to represent the network-ID and the last 64-bits are used to represent the interface-ID.

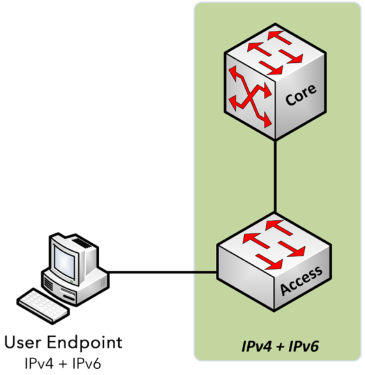
3.2.1 IPv6 Deployment

Select one (or more) of the following IPv6 Deployment PODs that will be used in the design:

	Deployment in LAN POD (Dual Stack)	**Deployment in LAN POD (ISATAP)**	**Deployment in WAN POD**
	Deployment in Internet POD	**Deployment in Internet POD (NAT64)**	

Deployment in LAN POD (Dual Stack)

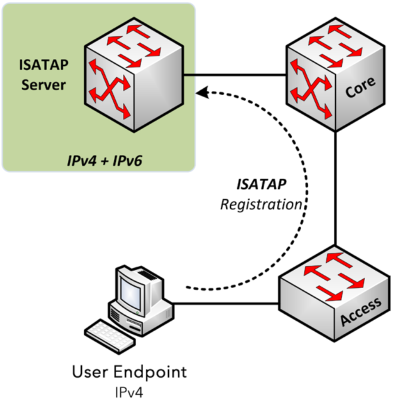
POD: IPV6-LAN1



- **When to use**: if you require running both IPv4 and IPv6 within the LAN/DC. This is the most common and recommended option compared to using ISATAP within the LAN.
- **Prerequisites**: LAN
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: LAN Core Switch & Access Switches
- **Description**: In this POD, each network device runs both protocol stacks (IPv4 and IPv6). Furthermore, the user endpoints (e.g. Microsoft Windows, Apple OS X, Linux) will also run IPv4 and IPv6 protocol stacks.

Deployment in LAN POD (ISATAP)

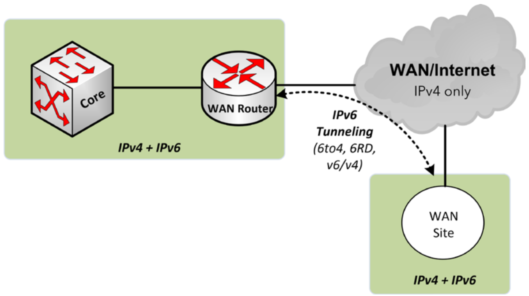
POD: IPV6-LAN2



- **When to use**: when most of the network hardware is IPv4 enabled. This will likely be for environments that are using older network hardware that doesn't support IPv6. Dual Stack is recommended over ISATAP.
- **Prerequisites**: LAN
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Core, Access, ISATAP device
- **Description**: In this POD, the user endpoints will be enabled for ISATAP. They will establish an ISATAP tunnel to a ISATAP server which may be the Core switch, distribution switch, or a dedicated switch handling all ISATAP services. The endpoint will be configured with a IPv4 address, but they will automatically be assigned an IPv6 address from the ISATAP server once the tunnel is established.

Deployment in WAN POD

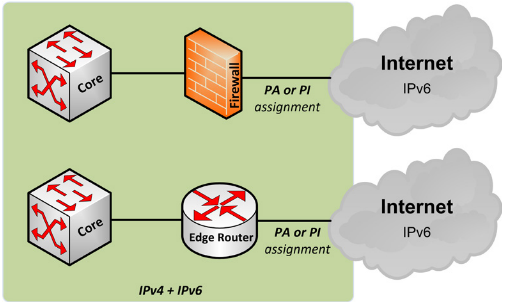
POD: IPV6-WAN



- **When to use**: if you require extending the IPv6 network over an existing IPv4 WAN that doesn't support IPv6
- **Prerequisites**: WAN
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: WAN router(s)
- **Description**: in this POD, the WAN routers are connected to an IPv4 WAN. The routers can be configured for IPv6 over IPv4 GRE, 6to4, or 6RD. These tunneling technologies do not provide data encryption and integrity services. 6to4 (or 6RD) is recommended to build automatic tunnels with other sites over an IPv4 network (Internet WAN or L3 WAN).

Deployment in Internet POD

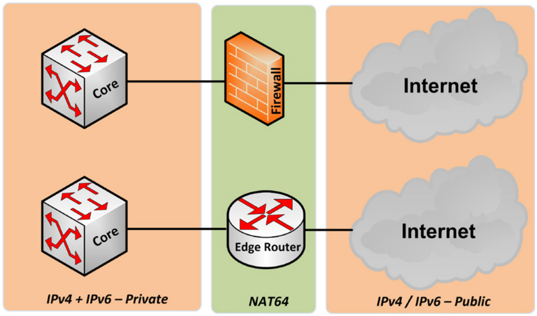
POD: IPV6-INET1



- **When to use**: if you require access to the IPv6 Internet from the IPv6 internal network.
- **Prerequisites**: INET
- **Required**: IPV6-ADD-GL or IPV6-ADD-INT-GL
- **Has Sub-PODs**: --
- **Components**: Edge router (or Firewall appliance)
- **Description**: in this POD, the edge router (or firewall appliance) are connected to an ISP enabled for IPv6 using global addressing. If the network will connect to a single ISP then a Provider Assigned (PA) global space is required. If the network will be connected to two (or more) ISPs then a Provider Independent (PI) global space is required.

Deployment in Internet POD (NAT64)

POD: IPV6-INET2



- **When to use**: if you require using private/internal IPv6 addressing for the endpoints. And then translating them to a Public IPv6 address on a supported edge router/firewall appliance in the Internet POD.
- **Prerequisites**: INET
- **Required**: IPV6-ADD-TR
- **Has Sub-PODs**: --
- **Components**: Edge router (or Firewall appliance)
- **Description**: in this POD, the edge router (or firewall appliance) is enabled for Stateful NAT64 using a Network Specific Prefix (NSP). NAT64 is used to allow communication between IPv4-only hosts and IPv6-only hosts by putting a translator between them. It performs IP header and address translation between the two protocol stacks.

Configuration

Below are required, recommended, and optional configuration when deploying IPv6 services:

Required

- **Hardware**: it requires using hardware that support IPv6 services
- **Addressing**: determine what addressing will be used for the endpoints and network devices internally on the network. This is determined in the two IPv6 Addressing PODs.

Deployment in WAN POD

- **Transition Technology**: determine what IPv6 transition technology will be used over the WAN. You can (1) implement ***IPv6 over IPv4 GRE tunnels*** for establishing point-to-point connections. You can implement (2) ***6to4*** to provide automatic tunneling among the WAN routers, but it requires using a 2002::/16 IPv6 prefix. Or you can implement (3) ***6RD*** to provide automatic tunneling among the WAN routers without any restrictions on what IPv6 prefix to use.
- **Deployment using 6to4**: if the WAN routers will be configured for 6to4 tunneling, it is required to use the 2002::/16 IPv6 prefix.

Deployment in Internet POD

- **Applications**: if FTP and SIP applications will be used through a NAT64 enabled device, it will require application-layer gateway (ALG) support for the translation
- **Global Addressing Assignment**: if you are using global addressing, determine what global addressing assignment will be used. This is based on how you obtain the global address space that will be used for your endpoints to access the Internet. Or to host network services that outside users can access from the IPv6 Internet. The address assignments include Provider Assigned (PA) and Provider Independent (PI).
- **Deployment using NAT64**: the NAT64 prefix in the Internet POD requires a Network Specific Prefix (NSP). This uses an organizational address space (global, unique-local, or site-local) which can be routable over the Internet if a global address is used.

Recommended (1/2)

- Do not use easily guessed interface-IDs like "DEADBEEF", "CAFE", or "C0FFEE" to ensure it isn't easily discovered in a network scan
- Disable route advertisements on point-to-point connections
- Tune the ARP table by setting the timeout to 200 seconds matching the MAC-address aging timer (default) which is 200 seconds
- Block the use of Microsoft Teredo
- Configure IPv6 VTY access controls to use the management (loopback) interface only
- Enable Neighbor Unreachability Detection (NUD)
- **SLAAC using SEND/CGA or EUI-64 with Stateless DHCPv6**: one of these options are recommended to provide dynamic addressing for the user endpoints when IP tracking and accounting capabilities is not required
- **Stateful DHCPv6**: this is recommended to provide dynamic addressing for the user endpoints when IP tracking and accounting capabilities is required

Recommended (2/2)

- **Blocking Hop-by-Hop and Routing Header Type 0 Packets**: it's recommended to block potentially malicious traffic that could be directed towards the network itself such as the Routing Header Type 0 (RH0) and the Hop-by-Hop (HbH) values that can be set in the IPv6 Extension Header.
- **/64 Prefixes**: this is recommended for user and server endpoints. This is required for SLAAC using SEND/CGA or EUI-64. Including ISATAP which embeds the IPv4 address in the last 32-bits of the IPv6 address. This prefix size is also used for the Embedded RP in IPv6 Multicast
- **/127 Prefixes**: this is recommended for point-to-point connections between network devices which can help against ping-pong network discovery attacks. This prefix size only accommodates two IPv6 addresses.
- **/128 Prefixes**: this is recommended for loopback addresses on network devices.

<u>Deployment in WAN POD</u>

- **Deployment using 6to4**: it is recommended to use 6to4 tunneling instead of using IPv6 over IPv4 tunnels which are not a scalable if there are dozens/hundreds of sites

<u>Deployment in Internet POD</u>

- **Global Assignment using Provider Assigned (PA):** when the network will be connected to a single ISP. The global address prefix is provided by the service provider that the network is connected to. The global address space can only be used with that service provider and no other provider. The biggest advantage for using this global assignment option is that the service provider would deal with the development and management of the address space that is used
- **Global Assignment using Provider Independent (PI):** when you require using a single global address space connecting to multiple service providers for Internet redundancy. In this global assignment, the global address space is provided by the regional registry (e.g. ARIN, RIPE, APNIC) that can be used between multiple service providers. It isn't tied directly to a specific service provider like the PA assignment. This allows an organization to switch to a different ISP without re-addressing all of the global nodes on the network.

Optional

- **IPv6 Prefix Guard**: a first-hop security protocol feature that blocks traffic from sourced IPv6 addresses that are outside the prefix gleaned from router advertisements

<u>Deployment in WAN POD</u>

- **Encryption**: the IPv6 tunneling protocols do not provide data encryption or integrity services with the established tunnels. Its recommended to implement IPsec with the tunnel to make it secure if that is required.

3.2.2 IPv6 Addressing - Network

Select one (or more) of the following IPv6 addressing PODs that will be used in the design:

Global IP Only	**Internal IP Only**	**Internal & Global IP**
Internal IP Translation to Global IP		

Global IP only

POD: IPV6-ADD-GL

- **When to use**: this is recommended for the endpoints. And if it is less likely you will change service providers and your global IPv6 address space.
- **Prerequisites**: IPV6-INET1
- **Description**: In this option, the endpoints are configured with a global IPv6 address allowing access to internal and external network resources without using a translation protocol. This option is recommended over the other PODs listed.

Internal IP only

POD: IPV6-ADD-INT

- **When to use**: this is recommended for internal devices that do not require Internet access such as printers, sensors, access-points, to engineering labs.
- **Prerequisites**: --
- **Description**: In this option, the node is configured with an internal/private IPv6 address. This can be a site-local or unique-local address (ULA), but a ULA is recommended between the two.

Internal & Global IP

POD: IPV6-ADD-INT-GL

- **When to use**: this is recommended if global IPv6 multicast and PMTUD services will be used on the IPv6 endpoint/device.
- **Prerequisites**: IPV6-INET1
- **Description**: In this option, the endpoint/device is configured with an internal IPv6 address for internal communication. And a global IPv6 address is assigned for external communication (e.g. Internet access). This option provides the most complexity from the other PODs listed due to several limitations.

Internal IP Translation to Global IP

POD: IPV6-ADD-TR

- **When to use**: this is recommended for (1) avoiding re-addressing all nodes if the global address space and service provider changes for an organization. Or (2) desired for pro-NAT network engineers who want to use private IPv6 addressing and use a IPv6 NAT protocol (e.g. NPTv6) to translate to a Public IPv6 address space for Internet access.
- **Prerequisites**: IPV6-INET2
- **Description**: In this option, the endpoints are configured with an internal IPv6 address (e.g. site-local or unique local). The edge router or firewall appliance would be configured with a translation protocol called NPTv6. The translation mechanism is stateless providing a 1:1 relationship between the internal addresses and the external addresses.

3.2.3 IPv6 Addressing – Interface-ID

Select one (or more) of the following IPv6 addressing PODs that will be used in the design:

	Static	**Dynamic using EUI-64**	**Dynamic using SEND/CGA**
	Dynamic using Privacy Extensions	**Dynamic using DHCPv6 (Stateful)**	**Dynamic using DHCPv6 (Stateless)**

Static

POD: IPV6-ID-ST

- **When to use**: this is ideal for servers and network infrastructure components (e.g. routers, switches, firewalls)
- **Prerequisites**: --
- **Description**: in this option, the interface-ID along with the network prefix is manually configured on the host.

Dynamic using EUI-64 (SLAAC)

POD: IPV6-ID-EUI

- **When to use**: if you require the IPv6 hosts to automatically generate its own Interface-ID without using a DHCP server in the environment. And don't require IP address tracking and accounting.
- **Prerequisites**: --
- **Description**: this is ideal for the following use-cases: (1) used for mobile environments. (2) Used for printers, sensors, and access points. Or (3) guest network where clients are connected for a short period of time. This dynamic option does not send DNS server and domain information to the IPv6 host. It requires stateless DHCPv6 to advertise those details.

Dynamic using SEND/CGA (SLAAC)

POD: IPV6-ID-SEND

- **When to use**: if you require the identity of the IPv6 host to be validated during the neighbor discovery process to protect against spoofing
- **Prerequisites**: --
- **Description**: the interface-ID is randomly generated. SEND/CGA is used to validate the identity of the nodes for the neighbor discovery process. For this process, it uses public/private keys and certificates to validate the identities of all nodes associated with the neighbor discovery process. This dynamic option does not send DNS server and domain information to the IPv6 host. It requires stateless DHCPv6 to advertise those details.

Dynamic using Privacy Extensions (SLAAC)

POD: IPV6-ID-PE

- **When to use**: if you require the Interface-ID to be randomly generated and used for a short period of time to avoid easy tracking of an IPv6 host on the network
- **Prerequisites**: --
- **Description**: the interface-ID is randomly generated and is used for a short period of time before a new pseudo random interface-ID is generated. Privacy extensions are used to address privacy concerns for tracking a IPv6 host when its interface-ID doesn't change in the case of the EUI-64 process. This dynamic option does not send DNS server and domain information to the IPv6 host. It requires stateless DHCPv6 to advertise those details.

Dynamic using DHCPv6 (Stateful)

POD: IPV6-ID-DHCP-SF

- **When to use**: if you require using a dedicated DHCP server to hand out IPv6 addresses, DNS, and domain information to endpoints on the network. And to provide user accounting and IP tracking capabilities.
- **Prerequisites**: --
- **Description**: In this dynamic option, a dedicated DHCPv6 server is responsible for handing out IPv6 addresses, DNS servers, and domain information to hosts on the network. This can provide many advantages such as tracking an IPv6 address and what is currently in use.

Dynamic using DHCPv6 (Stateless)

POD: IPV6-ID-DHCP-SL

- **When to use**: if you require advertising DNS and domain name information to hosts using EUI-64, SEND/CGA, or Privacy Extensions
- **Prerequisites**: IPV6-ID-EUI, IPV6-ID-SEND, or IPV6-ID-PE
- **Description**: this dynamic option is implemented with any of the SLAAC options (e.g. EUI-64) to dynamically provide DNS server and domain name information to the hosts.

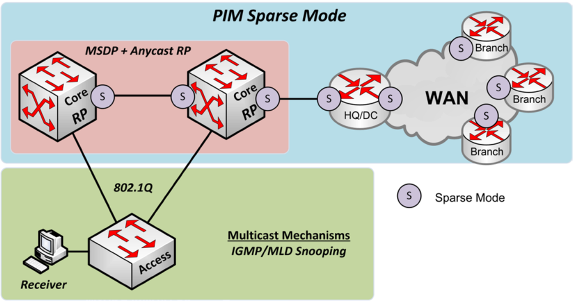
3.3 Multicast

Select one (or more) of the following Multicast PODs that will be used in the design:

	Deployment using PIM-SM (ASM)	**Deployment using Bi-Dir PIM (ASM)**	**Deployment using PIM-SSM (SSM)**

Deployment using PIM-SM (ASM)

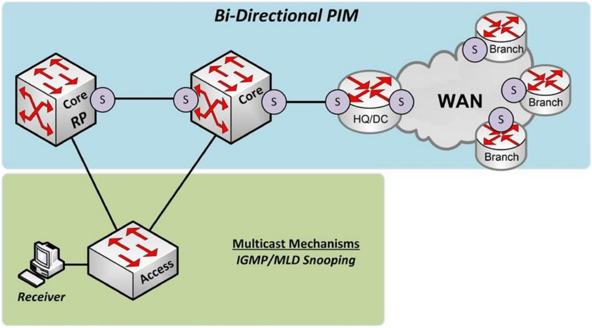
POD: MCAST-ASM-PIMSM



- **When to use**: (1) if the network will have a moderate use of multicast sources and receivers across the network such as voice services. (2) If you require support for IPv6 Multicast services. (3) If you require implementing Multicast redundancy.
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: RP (Core switch), Layer-3 devices (WAN routers, L3 Access switches)
- **Description**: PIM-SM uses an Any-Source Multicast (ASM) topology. In this POD, PIM Sparse Mode routing is implemented for the selected multicast groups across the LAN, DC, and WAN. The Core switch(s) are configured as the RP using either Auto-RP or Static RP. Multicast traffic would flow downstream from the RP towards the receivers that have requested to join a specific multicast group.

Deployment using Bi-Dir PIM (ASM)

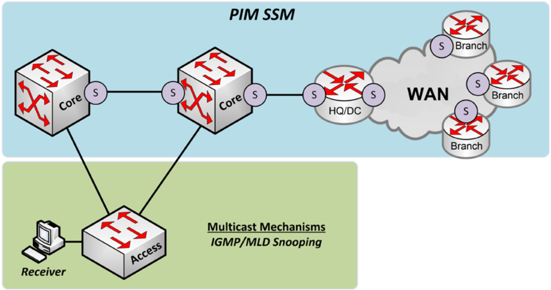
POD: MCAST-ASM-BIDIR



- **When to use**: if you require using a very scalable multicast domain to support thousands of receivers and sources sending multiple streams (many-to-many communication) in the environment
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: RP (Core switch), Layer-3 devices (WAN routers, L3 Access switches)
- **Description**: Bi-Directional PIM uses an Any-Source Multicast (ASM) topology. In this POD, Bi-Directional PIM is implemented for the selected multicast groups across the LAN, DC, and WAN. The Core switch(s) are configured as the RP using either Auto-RP or Static RP which is used as a key for Bi-Dir PIM. Multicast traffic can flow upstream and downstream throughout the network with multiple sources and receivers spread-out across the network.

Deployment using PIM-SSM (SSM)

POD: MCAST-SSM-PIM



- **When to use**: if you require (1) multicast receivers on the network to receive multicast traffic from a specific source/server that is streaming traffic. (2) The network has high traffic with one source streaming to many receivers. This can be audio/video streaming to Internet broadcasting. (3) If multicast services will be used over DMVPN and/or MPLS.
- **Prerequisites**: --
- **Required**: IGMPv3
- **Has Sub-PODs**: --
- **Components**: Layer-3 devices (WAN routers, L3 Core & Access switches)
- **Description**: PIM-SSM uses a Source-Specific Multicast (SSM) topology. In this POD, PIM-SSM is implemented across the LAN, DC, and WAN. Multicast receivers on the network can only receive multicast traffic from a specific source/server. When a receiver wants to receive specific traffic, they need to use the provided IP address of the Source/Server and the Multicast IP Address. This model does not build a shared tree nor requires a Rendezvous Point (RP). This offers more restrictions and security because the receiver has to specify which source/server it wants to receive data from. And not from any source/server that is streaming data across the network.

Configuration

Below are required, recommended, and optional configuration when deploying Multicast services:

Required

- **Positioning**: determine the location of all multicast source and receiver endpoints connected across the network.
- **Deployment using Any Source Multicast (ASM):** if you are using a PIM-SM or Bi-Directional PIM deployment, a Rendezvous Point (RP) is required for the topology.
- **Deployment using Source Specific Multicast (SSM):** if you are using a PIM-SSM deployment, it is required to implement IGMPv3 for the Group Management protocol in the topology. PIM-SSM also requires using 232.0.0.0/8 for the multicast address scope.

Recommended

- Use administratively scoped addresses (239.0.0.0/8) unless PIM-SSM is used which requires 232.0.0.0/8 addressing
- Tune PIM query internal timers to 1 second
- Use IP multicast boundaries to control where certain multicast traffic can go such as Wireless, WAN, and VPN networks.
- **Multicast Support at Layer-2**: it is recommended to enable IGMP snooping (using IPv4) and/or MLD snooping (using IPv6) on all switches with connected receivers attached. This mechanism will forward multicast traffic to the switch ports with connected receivers that have requested the multicast stream. This will free network resources and bandwidth on the switch.
- **Multicast Fast Drop (MFD)** should be enabled to rate limit non-RPF traffic. Many cases this is enabled by default.

<u>Deployment using Any Source Multicast (ASM)</u>

- **RP Placement**: it is recommended to implement the RP at the center of the network. This will likely be the Core switch in the topology.
- **RP IP Address**: it is recommended to use a loopback IP address for the RP address. It should be configured with a host address mask (32 bits).
- **Redundancy for PIM-SM**: it is recommended to setup MSDP and Anycast RP to provide RP redundancy (and load balancing) in the PIM-SM domain. MSDP and Anycast RP should be configured between the two LAN/DC Core switches in the topology.
- **RP for IPv4**: it is recommended to setup ***Auto-RP (or BSR)*** if new multicast services will be added to the network over time. This is used for multicast networks to provide dynamic RP management and is supported on networks using Cisco hardware. This is ideal for medium to large networks (including small or SMB) for better administration, flexibility, and scalability for managing the RP on Layer-3 devices on the multicast network. You can also use a ***Static RP*** among the routers if the multicast services will not change on the network.
- **RP for IPv6**: it is recommended to use ***BSR*** for delivering the RP-to-group mapping information within the LAN or Data Center. You can also use ***Embedded RP*** if IPv6 Multicast needs to be routed across domain boundaries such as remote sites.
- **RP using Auto-RP**: for Auto-RP tune the PIM RP announce internal timer to be between 3 to 5 seconds (default is 60 seconds)

Optional	• Keep multicast traffic on the shared path (optional). This will reduce the number of multicast states (S,G) from the leaf routers by keeping traffic on the shared tree • **Secure Multicast**: to secure multicast traffic using GDOI with IPsec encryption **<u>Deployment using Any Source Multicast (ASM)</u>** • **Rogue Source Protection**: optional security mechanism to allow what valid sources and multicast group addresses should register with the RP. • **Rogue RP Protection**: optional security mechanism to configure IGMP group access control to specify what multicast groups receivers can join. • **Auto-RP Protection**: optional security mechanism to configure an RP Announce Filter for valid RPs and multicast group addresses that should be used on the network.

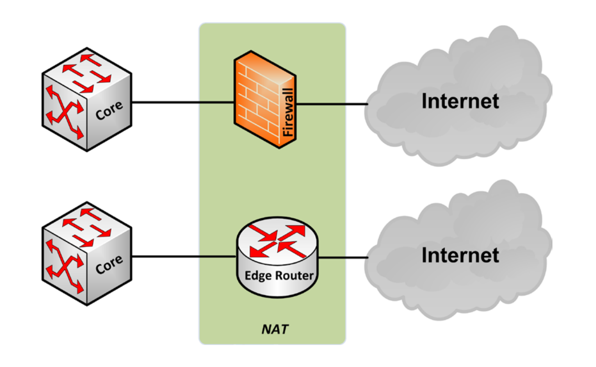
3.4 NAT

Select one (or more) of the following NAT PODs that will be used in the design:

	Deployment in Internet POD		

Deployment in Internet POD

POD: NAT-INET



- **When to use**: this is a standard deployment for NAT services used within the Internet POD
- **Prerequisites**: INET
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Edge Router or Firewall appliance
- **Description**: in this POD, NAT services will typically be deployed on the network device that is connected in-line between the internal/private network and the external/public network. Hence, the requirement to implement NAT to allow the internal network to access the Internet. Or hosts on the Internet accessing internal servers. Based on the Internet POD that is used, NAT services will either be deployed on the Edge router device or the Firewall appliance.

Configuration

Select one (or more) of the following NAT options that will be used:

	PAT / NAT Overload If you require the internal endpoints to access the Internet using the WAN IP from the edge router/firewall. Or using a dedicated Public IP address.	**NAT Port Forwarding** If you require mapping a single server on a particular port to another Public IP and port.	**Static NAT** If you require mapping a single server to a single Public IP.

Below are required, recommended, and optional configuring when deploying NAT services on the network based on the available options:

Required	• **Positioning**: determine where NAT will be implemented in the topology. This will likely be the edge router or firewall appliance that is located in the Internet POD. • **Hardware**: NAT services are only supported on router and firewall devices.

Recommended	• **Using PAT (or NAT Overload):** it is recommended to enable PAT for internal endpoints such as user and guest endpoints accessing the Internet. • **Using NAT Port Forwarding**: it is recommended to use this NAT option if you have a small set of Public IP addresses or only need a few ports (e.g. HTTPS, RDP) that need to be forwarded to a server. • **Using Static NAT**: it is recommended to use this NAT option if a wide range of services/ports will be used for translation to a single server. • **NAT with VPN**: it is recommended to disable NAT translations for networks that will be used over a VPN. Otherwise, all communication over the VPN tunnel will be translated. • **NAT Transparency (NAT-T):** it is recommended to allow support for NAT-T (or IPsec over UDP) to allow VPN clients to connect from behind a NAT-enabled device.

3.5 Operations

Below reflect the main categories for the operation PODs:

	User Specific	Network Specific	Vendor Specific		

User Specific

Select one (or more) of the following user specific services that will be used:

	DHCP	DNS	

DHCP

POD: OPS-DHCP

- **When to use**: if you require endpoints to obtain their IP address automatically from a server (or network device)
- **Prerequisites**: LAN
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: it is recommended to use a dedicated DHCP server for medium and large sized networks. DHCP server enabled on network devices is common for smaller sized networks. Create all of the DHCP scopes required to include the address pool, DNS server(s), lease, and any specific options (e.g. phone system, wireless, etc.)

DNS

POD: OPS-DNS

- **When to use**: if you require endpoints accessing the Internet or network resources using domain names
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: a public (or external) DNS server can be used if the site doesn't require accessing internal endpoints by name. An internal DNS server can be deployed if the site requires accessing internal endpoints by name. The internal DNS server can also be configured to use an external DNS server as DNS forwarders to handle DNS requests for Internet-based websites.

Network Specific

Select one (or more) of the following network specific services that will be used:

DHCP Forwarding	**Flow Control**	**Jumbo Frames**
NTP	**NetFlow**	**Port Monitor**
RADIUS/TACACS+/LDAP	**SNMP**	**Syslog**
WCCP	**Dynamic DNS (DDNS)**	**Port Channel / 802.3ad**

DHCP Forwarding

POD: OPS-DHCPFWD

- **When to use**: this is required if the DHCP server is located on a different network from where the user endpoints are located
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: if there are several networks (e.g. User, Server, Guest) that exist, DHCP forwarding such as IP helper (Cisco IOS) would be enabled on the Layer-3 interface for the DHCP enabled networks. It would point to the DHCP server(s). IP helper will forward DHCP broadcast requests to the server listed in the IP helper (e.g. DHCP server).

Dynamic DNS (DDNS)

POD: OPS-DDNS

- **When to use**: if you have public facing servers (or routers) that need to be accessed from the Internet, but the site is using a dynamic IP address (via DHCP or PPPoE) that will regularly change
- **Prerequisites**: INET
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: a dynamic DNS service where a host (or router) is configured for DDNS. It would connect periodically to a DDNS provider to register its current IP address. DDNS can be used to update its current IP with a DNS record automatically.

Netflow

POD: OPS-NF

- **When to use**: if you want to view top-talker information based on the IP address and applications recorded from traffic flows through a network device. Other use-cases include network planning and billing purposes.
- **Prerequisites**: --
- **Required**: Cisco Router (Netflow)
- **Has Sub-PODs**: --
- **Description**: when configuring NetFlow it is important to know what version (plus if it is supported) will be used. It is recommended to use version 9 which provides the most flexibility with exporting Netflow data that has been collected. You can also enable the “top-talker” feature to view top bandwidth users. It can also be used to track general traffic patterns for monitoring and troubleshooting purposes.

NTP

POD: OPS-NTP

- **When to use**: recommended protocol that should be enabled on all network devices to pull their date and time from a time server for accurate timestamps
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: it is recommended to use a reliable time server source such as the NIST Internet Time Server (time.nist.gov).

Port Monitor

POD: OPS-SPAN

- **When to use**: a feature that allows capturing packets from specified ports and sending the traffic to a network analyzer/sniffer/tap device
- **Prerequisites**: --
- **Required**: Hardware (Switch)
- **Has Sub-PODs**: --
- **Description**: There are several port monitoring mechanisms that can be used on the network depending on what is supported on the network switch. There is SPAN (most common) which does port monitoring on the local switch it is configured on. There is RSPAN which does port monitoring across a Layer-2 network using a dedicated VLAN. And there is ERSPAN which does port monitoring across a Layer-3 network.

RADIUS / TACACS+ / LDAP

POD: OPS-AUTH

- **When to use**: if you want to use a network authentication protocol to provide centralized authentication for access to network devices
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: TACACS+ is supported on Cisco network devices and RADIUS is an industry standard protocol that can be used (recommended over TACACS+) to provide network authentication. An alternative option would be using the existing AD domain (using LDAP) which can be integrated to work with supported network devices (e.g. Firewalls).

SNMP

POD: OPS-SNMP

- **When to use**: used for monitoring a network device's performance and operational status including other statistics
- **Prerequisites**: NM-NMS
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: SNMPv3 is recommended to provide increased security over SNMPv2c which uses clear-text for all communication. SNMPv3 provides encryption for all communication between the network device and the NMS system.

Syslog

POD: OPS-SYSLOG

- **When to use**: used for recording system and log events that can be stored locally or sent to a Syslog server
- **Prerequisites**: NM-NMS
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: this is recommended to be implemented on all network devices. This allows system/security related events to be sent to a centralized log server, so when there is an issue, you can look at the logs based on the timestamp.

Jumbo Frames

POD: OPS-JUMBO

- **When to use**: if you require the network to support large packet sizes (MTU 9000 bytes) typically used with an Ethernet SAN (using iSCSI)
- **Prerequisites**: DC, SAN (SAN-ISCSI or SAN-FCOE-ISCSI)
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: this feature is typically deployed globally on a switch to allow support of Jumbo frames if they are used by the servers and storage arrays devices. Increasing the MTU can increase performance for bulk data transfers.

Flow Control

POD: OPS-FC

- **When to use**: if you are using high-performing servers and want to prevent network drops
- **Prerequisites**: DC, SAN (SAN-ISCSI or SAN-FCOE-ISCSI)
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: this feature is implemented on switch ports with high-performing systems attached such as an ISCSI storage array.

WCCP

POD: OPS-WCCP

- **When to use**: a protocol used with a proxy or WAN optimization solution to transparently send traffic to an optimization or proxy appliance
- **Prerequisites**: OPT-WAN
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: Used to transparently send traffic (e.g. HTTP, FTP) to an optimization/proxy appliance. This service is usually implemented on the WAN router (or Core switch) in the topology depending on how the solution is deployed.

Port Channel / 802.3ad

POD: OPS-PC

- **When to use**: if you require bundling multiple interfaces to appear as one logical interface to provide increased bandwidth resources
- **Prerequisites**: LAN/DC
- **Required**: --
- **Has Sub-PODs**: Go to 3.5.1
- **Description**: you can bundle up to 8 interfaces/ports to appear as a single interface. It's recommended to bundle interfaces in multiples of 2 within a port channel group. Furthermore, a Port Channel can provide sub-second failover between links in a configured bundle. See the Port Channel POD for further design planning and details.

Vendor Specific - Cisco

Select one (or more) of the following Cisco specific services that will be used:

BIDI	**Breakout**	**CoPP**
Embedded Packet Capture	**EPLD**	**EEM**
GOLD	**ISSU**	**NSF/SSO**
StackWise	**StackPower**	**VDC**
VPC	**VSS**	**Cisco Medianet**

BIDI

POD: OPS-CSCO-BIDI

- **When to use**: if you want to allow a 40GE to run over a single pair of multi-mode OM3 fiber
- **Prerequisites**: --
- **Required**: Cisco Nexus 7K
- **Has Sub-PODs**: --
- **Description**: reduces cabling requirements for 40GE connections. BIDI optics are supported on Nexus 7000/7700 F3 and M2 series modules

Breakout

POD: OPS-CSCO-BOUT

- **When to use**: if you want to take a 40GE port and configure it as four individual 10GE ports
- **Prerequisites**: --
- **Required**: Cisco Nexus 7K
- **Has Sub-PODs**: --
- **Description**: You can configure a 40GE port to be used as four independent 10GE interfaces. No reload or reset is required for any of the components when you enable breakout. These interfaces can be configured as routed ports, switch ports, port channels or FEX interfaces.

Control Plane Policing (CoPP)

POD: OPS-CSCO-COPP

- **When to use**: if you want to rate-limit traffic that goes to the CPU of the network switch/router
- **Prerequisites**: --
- **Required**: Cisco Router / Switch
- **Has Sub-PODs**: --
- **Description**: applies hardware QoS policies to traffic punted to the CPU. This can help against reconnaissance and DoS attacks to the Control Plane of the Cisco network devices.

Embedded Packet Capture

POD: OPS-CSCO-EPC

- **When to use**: if you want a feature that can perform packet captures directly on a network device
- **Prerequisites**: --
- **Required**: Cisco Router
- **Has Sub-PODs**: --
- **Description**: a feature that can perform packet captures directly on a supported Cisco Router storing them in the DRAM. It is recommended to setup filters to capture certain traffic flows through the router.

EPLD

POD: OPS-CSCO-EPLD

- **When to use**: a Nexus feature that provides hardware functionality to the I/O modules
- **Prerequisites**: --
- **Required**: Cisco Nexus 7K
- **Has Sub-PODs**: --
- **Description**: EPLD upgrades is a separate and independent process from ISSU. The upgrade is disruptive to traffic hence the module must be powered down during upgrade. Lastly, EPLD upgrades are not always required. It is recommended to view the EPLD release notes for more information.

EEM

POD: OPS-CSCO-EEM

- **When to use**: a feature that can monitor key system components such as CPU utilization, interface errors, counters, SNMP, and SYSLOG events
- **Prerequisites**: --
- **Required**: Cisco Nexus 7K
- **Has Sub-PODs**: --
- **Description**: Cisco IOS technology that runs on the control plane. It is a combination of processes designed to monitor key system parameters such as CPU utilization, interface errors, counters, SNMP, and SYSLOG events.

GOLD

POD: OPS-CSCO-GOLD

- **When to use**: an operational feature that can check the health of the hardware components. It can verify the operation of the system's data plane and control plane at run-time including boot-time.
- **Prerequisites**: --
- **Required**: Cisco Catalyst 4K, 6K
- **Has Sub-PODs**: --
- **Description**: common framework to check the health of the hardware components and verify proper operation of the system data plane and control plane.

In-Service Software Upgrade (ISSU)

POD: OPS-CSCO-ISSU

- **When to use**: a feature that allows doing an OS upgrade on a Cisco switch without bringing down the entire switch
- **Prerequisites**: --
- **Required**: Cisco Nexus 7K, Catalyst 4K, 6K
- **Has Sub-PODs**: --
- **Description**: this is a software capability that allows doing an OS upgrade on Cisco L3-switches without bringing down the entire switch. It allows for a new software version to be tested and verified before completing an upgrade to a Cisco switch. Full image ISSU requires a dual supervisor environment which is well suited for single points of failure at the access layer.

NSF/SSO

POD: OPS-CSCO-NSF

- **When to use**: a recommended feature that should be implemented on supported hardware to provide fast switchover between supervisor engines in a chassis-based switch
- **Prerequisites**: --
- **Required**: Cisco Catalyst 6K, 4K
- **Has Sub-PODs**: --
- **Description**: SSO provides fast transparent data plane switchover when there is a hardware failure. It can synchronize its active processes and configuration between two redundant supervisor engines inside of a supported Cisco Catalyst chassis-based switch. If a failure occurs, the NSF/SSO convergence time is between 1-3 seconds, but the links are not dropped and no convergence occurs on the network. Furthermore, some features and protocols may be NSF-aware like HSRP.

StackWise

POD: OPS-CSCO-STW

- **When to use**: if you require using a stack-based Cisco Catalyst 3700 series switch in the environment
- **Prerequisites**: LAN-1T-C/S, LAN-2T-C/S, DC-1T-C/S, or DC-2T-C/S
- **Required**: Cisco Catalyst 3750 series
- **Has Sub-PODs**: --
- **Description**: Cisco StackWise Plus is supported on a selected number of Cisco Catalyst switches which can stack up to 9 switches with sub-second failure recovery.

StackPower

POD: OPS-CSCO-STPWR

- **When to use**: if you require sharing power across a stack of Cisco Catalyst 3750 switches used in the environment
- **Prerequisites**: LAN-1T-C/S, LAN-2T-C/S
- **Required**: Cisco Catalyst 3750-X series
- **Has Sub-PODs**: --
- **Description**: provides capability of sharing power across a stack of Cisco Catalyst 3750-X switches for flexibility to use all power supplies available in the stack.

VDC

POD: OPS-CSCO-VDC

- **When to use**: if you require creating several virtual switches on Cisco Nexus hardware
- **Prerequisites**: --
- **Required**: Cisco Nexus 7K
- **Has Sub-PODs**: --
- **Description**: you can create up to four logical switches. The default VDC on the Nexus switch is 1. Each VDC runs its own independent processes to prevent performance issues in other VDCs.

VPC

POD: OPS-CSCO-VPC

- **When to use**: a feature that allows building a port channel between two Cisco Nexus switches to appear as one logical port channel connection
- **Prerequisites**: DC-2T-PHY-VPC or DC-2T-UNF-VPC
- **Required**: Cisco Nexus
- **Has Sub-PODs**: Go to 3.5.2
- **Description**: VPC can be implemented down to DC access switches. Or with servers connected off of the DC access switches in the topology (called Enhanced VPC). There is also extended VPC support for Data Center networks using FabricPath called VPC+. See the VPC PODs for further design planning and details.

VSS

POD: OPS-CSCO-VSS

- **When to use**: an advanced feature that can make two physical switches appear as one logical switch
- **Prerequisites**: LAN-2T-PHY-VSS
- **Required**: Cisco Catalyst 6K, 4K
- **Has Sub-PODs**: Go to 3.5.3
- **Description**: VSS is typically implemented on the LAN Core switches to appear as one logical switch. VSS does not rely on STP and is limited to be configured between only two switches. If a Port Channel is configured between the two VSS switches to a single access switch, the access switch will assume it is really peering with a single switch increasing the overall availability for the connected hosts on the switch. See the VSS PODs for further design planning and details.

Cisco Medianet

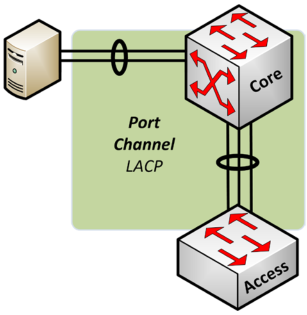
POD: OPS-CSCO-MN

- **When to use**: optional Cisco feature recommended for networks enabled for Voice and Video solutions
- **Prerequisites**: COL
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: Cisco Medianet has many capabilities such as media monitoring and awareness to provide increased visibility for the voice engineer. It can also provide proactive management and troubleshooting of network resources. The Cisco Medianet media monitoring capabilities consist of Performance Monitor, Mediatrace, and using the IP SLA Video Operation (VO). The Cisco Medianet media awareness capabilities consist of Flow Metadata, the Media Services Interface (MSI), and the Media Services Proxy (MSP).

3.5.1 Port Channel (802.3ad)

Select one (or more) of the following Port Channel PODs that will be used in the design:

	Deployment in LAN/DC		

Deployment in LAN/DC
POD: OPS-PC-STD


- **When to use**: this is the standard deployment for Port Channels within the LAN and/or DC topology
- **Prerequisites**: LAN/DC
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Port Channel-capable device (Switches, Routers, Firewalls, Servers)
- **Description**: in this POD, a Port Channel (enabled for LACP) would be built between two devices. This can be network devices such as routers, firewalls, and switches. Or even with a server with the appropriate hardware.

Configuration

Below are required, recommended, and optional configuration when deploying Port Channel services.

Required

- **Negotiation Protocol**: determine what port channel protocol will be used for bundling multiple interfaces and building a port channel with the neighboring device. The negotiation protocols include LACP (industry standard) and PAgP (Cisco).
- **Layer-2 or Layer-3 Port Channel**: depending on the connections used on the LAN/Data Center network, determine if the Port Channel interface will be a Layer-2 or Layer-3 connection

Recommended

- **Negotiation Protocol using LACP**: recommended protocol to use since it is an industry standard protocol that can be used with Cisco and other vendor devices. This can include dual-homed servers that may need to be port channeled to the Data Center switch. LACP can also support a higher number of interfaces that can be bundled together.
- **Load Balance Hash**: a port channel is really load balancing between multiple interfaces that are bundled together. The recommended hash algorithm to use for the port channel bundle is “src-dst-ip” or “src-dst-port” depending on what hash algorithm is supported on the hardware.

Optional

- None Available

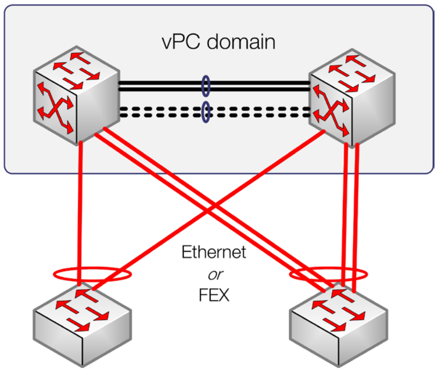
3.5.2 Virtual Port Channel (VPC)

Select one (or more) of the following VPC PODs that will be used in the design:

	Multi-Chassis EtherChannel (MEC)	**Enhanced VPC**	**VPC+**

Multi-Chassis EtherChannel (MEC)

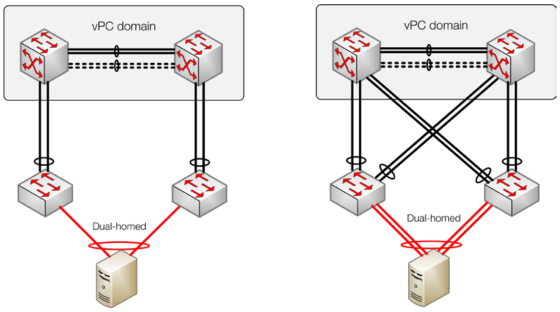
POD: OPS-CSCO-VPC-MEC



- **When to use**: if you require building a port channel between two Cisco Nexus switches to appear as one logical port-channel connection to a DC access switch
- **Prerequisites**: DC-2T-PHY-VPC or DC-2T-UNF-VPC
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: VPC peers (DC Core switches), DC access
- **Description**: in this POD, VPC would be configured between two DC core switches. The DC access switch (using either Ethernet or FEX connections) would build a Port Channel between the two VPC peers as shown in the picture above. This configuration is called a Multi-Chassis EtherChannel (MEC). The DC access switches can have multiple uplinks in the port channel with the VPC peers to provide minimal resiliency. It is recommended to use two Ethernet or FEX uplinks to the VPC core.

Enhanced VPC

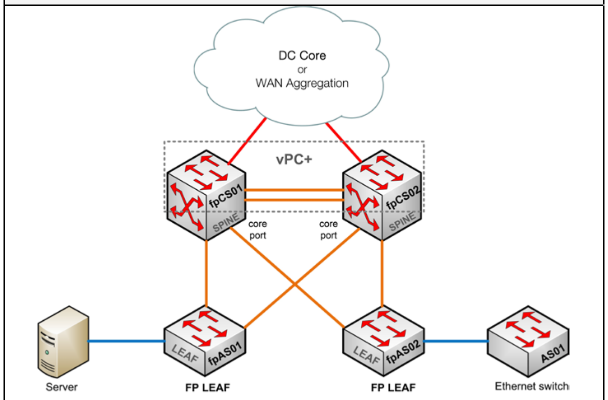
POD: OPS-CSCO-VPC-ENH



- **When to use**: if you require extending VPC down to the DC access layer to allow servers to be dual-homed between two DC access switches
- **Prerequisites**: DC-2T-PHY-VPC or DC-2T-UNF-VPC
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: VPC peers (DC Core switches), DC Access, Servers
- **Description**: in this POD, VPC would be configured between two DC core switches. The DC access switch (using either Ethernet or FEX connections) would build Port Channels with one (or both) of the VPC peers. The server would be dual-homed between two of the DC access switches as seen in the picture above. This configuration is called an Enhanced VPC since the VPC functions are pushed down to the DC access layer in the topology. It is recommended to use two Ethernet or FEX uplinks to the VPC core.

VPC+

POD: OPS-CSCO-VPC+



- **When to use**: if the DC will use a Spine-Leaf CLOS topology with FabricPath routing
- **Prerequisites**: DC-CLOS, OVR-FP
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: in this POD, FabricPath is enabled between the Spine and Leaf switches. The Spine (or Border) switches will be configured in a VPC+ domain.

Configuration

Below are required, recommended, and optional configuration when deploying VPC services.

Required	• **Hardware**: it requires using Cisco Nexus hardware, modules (Supervisor Engine, Line modules), and OS software that support VPC • **Licensing**: to enable the use of VPC on a Cisco Nexus switch it requires the appropriate license to be activated • **Services**: it is required to implement UDLD, Port Channel, Bridge Assurance, and a FHRP when deploying VPC • **vPC Domain**: it is required to define a single vPC domain that will include the two vPC enabled devices, the vPC peer link, the vPC peer keepalive link, and all of the Port Channels created from the two vPC peers. • **vPC Peer Link**: it is required to define an interface that will be used between the vPC peer devices for synchronizing control plane traffic. You should have at least two 10-Gigabit Ethernet interfaces for the peer link. • **vPC Peer Keepalive Link**: this is more of a recommendation, but also define a dedicated interface that will be used to monitor the health of the other vPC peer by sending periodic keepalive messages. No data traffic is synchronized over this link. • **Layer-2 Connection for DC Access**: it is required to configure Layer-2 vPC connections between the VPC peers (Core layer) and the DC access switches.

Recommended	• **Priority**: it is recommended to define which VPC switch in the domain will be the active/primary switch. The default priority value is 32,768. It is recommended to configure a lower priority value, such as 16000, on the VPC switch that will be the active switch in the domain. • It is recommended to enable “**auto-recovery**” on the VPC peers to increase resiliency • **Maximum Fabric Uplinks**: it is recommended to configure the maximum number of fabric uplinks using either Twinax (CX-1) cabling or Fabric Extender Transceivers (FET) with OM3 multi-mode fiber • **Storage with Enhanced VPC**: if EtherChannel servers will use FCoE, the storage traffic must be isolated and cannot connect to both Core switches. • **Multicast**: an unused VLAN for IP Multicast (“bind-vrf”) replication synchronization should be used between the vPC switches. This VLAN cannot appear in the configuration, VLAN database, nor included in any Trunk security list. It will automatically setup packet replication across the vPC peer link when needed.

Optional	• **Object Tracking**: an optional vPC feature that can monitor the state of critical interfaces on the Data Center Core (using Cisco Nexus 5500). It can track interfaces and perform an action which could relinquish vPC domain control to the other vPC switch. This requires implementing a vPC peer keepalive link within the vPC domain. Enabling this feature is recommended if the Data Center vPC Core will connect to a LAN Core. Object tracking would be enabled on the physical ports that connect into the LAN Core switch.

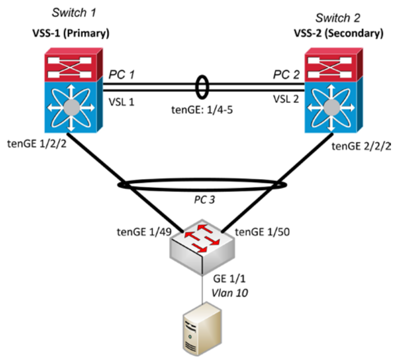
3.5.3 Virtual Switching System

Select one of the following VSS PODs that will be used in the design:

	Deployment in LAN POD		

Deployment in LAN POD

POD: OPS-CSCO-VSS-STD



- **When to use**: this is the standard deployment for VSS among the two Core switches in the LAN
- **Prerequisites**: LAN-2T-PHY-VSS
- **Required**: Hardware (Cisco Catalyst 6K)
- **Has Sub-PODs**: --
- **Components**: VSS Domain (LAN Core switches)
- **Description**: in this POD, redundant LAN core switches are clustered together to appear as one logical switch using VSS. Port Channel can be implemented from the two redundant Core switches to each access switch increasing the overall availability for the connected hosts on the access switch as shown in the picture above. The access switch will assume it is connected to a single Core switch.

Configuration

Below are required, recommended, and optional configuration when deploying VSS services.

Required	• **Hardware**: connect two Cisco Catalyst switches (e.g. Cisco Catalyst 6500 VSS 4T) together using 10GE connections supporting VSS to provide the Virtual Switch Link (VSL). • **VSS Domain & Switch ID**: define a unique domain shared by both switches including a unique number (e.g. switch ID) for each switch in the VSS domain • **VSL Link**: configure a VSL link between the two VSS switches. The VSL allows the supervisors to communicate using SSO redundancy to keep the control plane synchronized between the two supervisor engines. To build the VSL, use unique port channel numbers on each VSS switch. • **Virtual Mode Operation**: enable the virtual mode operation which will renumber the interfaces to the format of “interface [switch number]/[module number]/[interface on module]”. Doing this operation will reboot both of the switches and the standby switch will display a "Standby" prompt.

Recommended	• **Dual-Active Detection Mechanism**: setup Dual-Active detection mechanism using Fast Hello (VLSP) between the two VSS switches. If the VSL link fails, both supervisors would resume the active control plane role creating a dual-active condition. To prevent dual-active scenarios, VSS supports a dual-active detection mechanism which will trigger VSS recovery mode. In VSS recovery mode, only one supervisor is allowed to remain active while the supervisor on the other VSS switch goes into recovery mode. As a result, the VSS switch in recovery mode will shut down all of its interfaces except for the VSL link to prevent instability. Once the VSL is restored, VSS would reload the switch that was in recovery mode and return to a normal operating mode. Fast Hello (VLSP) is recommended using a GE interface between the two VSS switches. This detection link is used for exchanging control plane hello messages between the two switches. • **Virtual MAC Address**: by default, the active switch in the VSS domain uses the default chassis-based MAC address pool assigned to the switch. It’s recommended to set a virtual MAC address for the VSS system, so that either active supervisor in the domain will use the same MAC address pool. • **VSS Quad Supervisor SSO (VS4O):** recommended on LAN Core switches using Cisco Catalyst 6800 series hardware

Optional	• **Enhanced Fast Software Upgrade (EFSU):** provides the capability to upgrade IOS software on the VSS Cisco Catalyst 6K switches. It is based on ISSU allowing support to perform IOS upgrades without downtime. ISSU allows VSS to maintain 50% of bandwidth during software upgrade. It also allows for different images to run on the Active and Standby Supervisor Engines.

3.6 Overlay / Tunneling

Select one (or more) of the following overlay/tunneling services that will be used in the design:

OTV	**LISP**	**VXLAN**
NVGRE	**OTP**	**FabricPath**

OTV

POD: OVR-OTV

- **When to use**: if you need to extend VLANs across a WAN with other data centers
- **Prerequisites**: DC, WAN
- **Required**: Routers/L3-Switches
- **Has Sub-PODs**: Go to 3.6.3

LISP

POD: OVR-LISP

- **When to use**: a naming service used by routers to get routing information for reaching other sites (or Data Centers)
- **Prerequisites**: DC, WAN
- **Required**: Routers/L3-Switches
- **Has Sub-PODs**: Go to 3.6.2

VXLAN

POD: OVR-VXLAN

- **When to use**: used in a IaaS environment with a large number of virtualized customer networks to scale beyond VLANs (4000+)
- **Prerequisites**: DC-CLOS
- **Required**: Routers/L3-Switches
- **Has Sub-PODs**: Go to 3.6.5

NVGRE

POD: OVR-NVGRE

- **When to use**: an alternative to VXLAN which uses GRE to tunnel Layer-2 packets over a Layer-3 network
- **Prerequisites**: DC
- **Required**: Routers/L3-Switches
- **Has Sub-PODs**: --

FabricPath

POD: OVR-FP

- **When to use**: to provide Layer-2 routing and load-balancing (ECMP) within a Spine-Leaf topology using Cisco hardware
- **Prerequisites**: DC-CLOS
- **Required**: Cisco Nexus hardware
- **Has Sub-PODs**: Go to 3.6.1

Over the Top (OTP)

POD: OVR-OTP

- **When to use**: if you require using WAN routers running EIGRP over the Internet without using VPN tunnels
- **Prerequisites**: DC, WAN
- **Required**: RT-EIGRP
- **Has Sub-PODs**: --

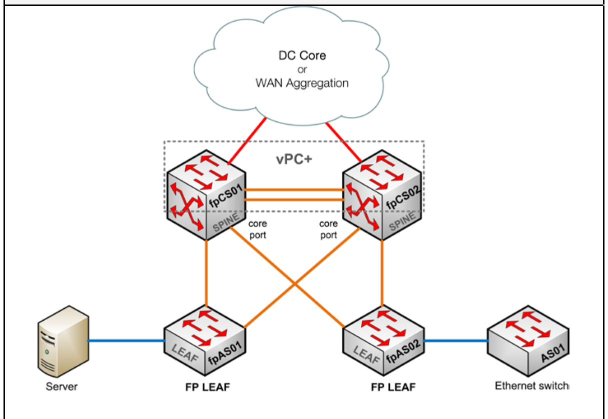
3.6.1 FabricPath

Select one (or more) of the following FabricPath PODs that will be used in the design:

	Deployment with Dual Spines	**Deployment with Multiple Spines**	**Deployment with Border**
	Deployment with Super-Spine & Border		

Deployment with Dual Spines

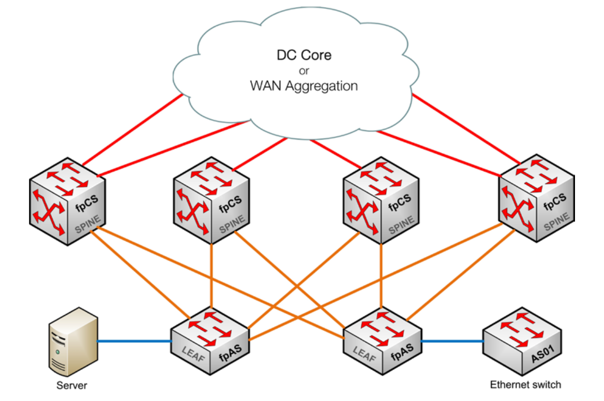
POD: OVR-FP-DUAL



- **When to use**: if the DC is using a Spine-Leaf CLOS topology with dual Spine switches providing access to the WAN, Internet, and/or Traditional DC
- **Prerequisites**: DC-CLOS
- **Required**: Cisco Nexus, OPS-CSCO-VPC+
- **Has Sub-PODs**: --
- **Description**: in this POD, FabricPath is enabled on the interfaces (core ports) between the Spine and Leaf switches. The Leaf switches will have servers and/or Ethernet switches attached (e.g. Cisco Nexus FEX). Connected off of the Spine layer will be access to other network solutions such as WAN, Internet, LAN, to even a Traditional DC. The Spine switches will be configured in a VPC+ domain including all VLAN SVI defined.

Deployment with Multiple Spines

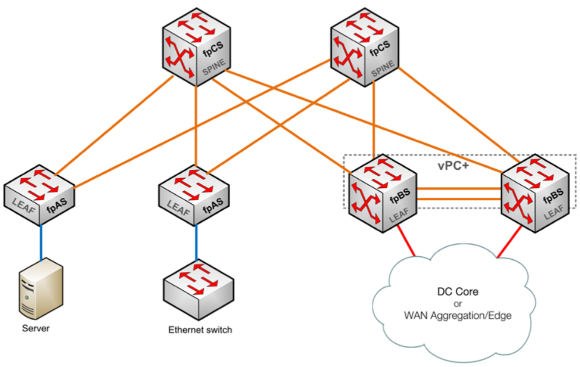
POD: OVR-FP-MUL



- **When to use**: if the DC is using a Spine-Leaf CLOS topology with 3-4 Spine switches providing access to the WAN, Internet, and/or Traditional DC
- **Prerequisites**: DC-CLOS
- **Required**: Cisco Nexus, OPS-CSCO-VPC+
- **Has Sub-PODs**: --
- **Description**: in this POD, FabricPath is enabled on the interfaces (core ports) between the Spine and Leaf switches. The Leaf switches will have servers and/or Ethernet switches attached (e.g. Cisco Nexus FEX). Connected off of the Spine layer will be access to other network solutions such as WAN, Internet, LAN, to even a Traditional DC. The Spine switches will be configured for Anycast HSRP.

Deployment with Border

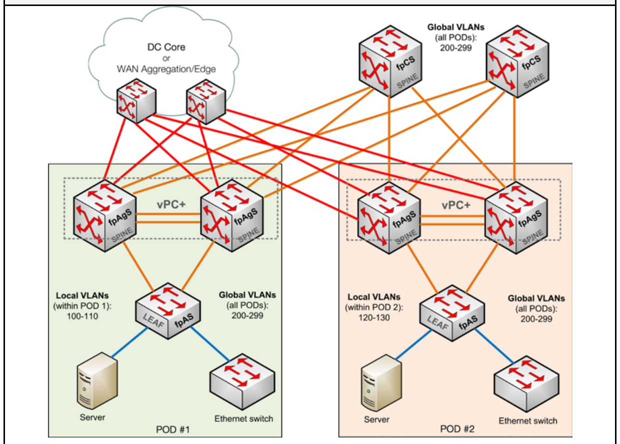
POD: OVR-FP-B



- **When to use**: if the DC is using a Spine-Leaf CLOS topology with a Border CLOS add-on to provide access to the WAN, Internet, and/or Traditional DC
- **Prerequisites**: DC-CLOS, DC-CLOS-B
- **Required**: Cisco Nexus, OPS-CSCO-VPC+
- **Has Sub-PODs**: --
- **Description**: in this POD, FabricPath is enabled on the interfaces (core ports) between the Spine, Leaf, and Border switches. The Leaf switches will have servers and/or Ethernet switches attached (e.g. Cisco Nexus FEX). The Border switch will provide access to other network solutions such as WAN, Internet, LAN, to even a Traditional DC. The Border switches will be configured in a VPC+ domain including all VLAN SVI defined as shown in the picture above.

Deployment with Super-Spine & Border

POD: OVR-FP-SS-B



- **When to use**: if the DC is using multiple Spine-Leaf CLOS PODs connected to a Super-Spine and using a Border CLOS add-on to provide access to the WAN, Internet, and/or Traditional DC
- **Prerequisites**: DC-CLOS, DC-CLOS-SS, DC-CLOS-B
- **Required**: Cisco Nexus, OPS-CSCO-VPC+
- **Has Sub-PODs**: --
- **Description**: in this POD, FabricPath is enabled on the interfaces (core ports) between the Spine and Leaf in each POD including the Super-Spine as shown in the picture above. The Spine switches in each of the PODs would have Layer-3 interfaces up to the Border switches. The Leaf switches (in each POD) will have servers and/or Ethernet switches attached (e.g. Cisco Nexus FEX). The Border CLOS will provide access to other network solutions such as WAN, Internet, LAN, to even a Traditional DC. Each of the Spine switches will be configured in a VPC+ domain and for all VLAN SVI used within that local Spine-Leaf POD.

Configuration

Below are required, recommended, and optional configuration when deploying FabricPath services:

Required	• **Hardware**: it requires using Cisco hardware that support FabricPath such as the Nexus 5500, 6000, and 7000 series. • **Positioning**: determine where FabricPath will be implemented in the topology. It will be deployed among the Data Center Spine and Leaf switches in a Spine-Leaf CLOS to provide Layer-2 routing capabilities. • **Licensing**: to enable the use of FabricPath on a Cisco Nexus switch it requires the Enhanced Layer 2 license to the activated. • FabricPath feature must be enabled on the default and non-default VDC

Recommended	• Configure the switch ID manually on all FabricPath switches • FabricPath VLANs must be configured on all switches in the FabricPath domain • Use the default reference bandwidth (400Gbps). FabricPath will always take the path with the lowest metric through the FabricPath domain. • Do not use UDLD • Disable IP redirects on all VLAN SVIs • Use passive interfaces on VLAN SVIs to avoid any routing adjacencies occurring • **Fast Convergence**: tune Layer-2 IS-IS SPF and LSP timers to provide fast convergence if there is a failure within the FabricPath topology. The timers should be tuned to 50msec (for the initial wait and second wait timers). • Disable IS-IS hello padding on the Cisco Nexus 7000 (if applicable) when jumbo frames is enabled • The MAC timer should be consistent on all devices in the Layer-2 topology • Make the FabricPath Leaf switch the primary root bridge for all VLANs that are used within the Ethernet domain that it is connected to • Use port channels between the FabricPath switches to decrease the number of direct IS-IS adjacencies. • Configure the highest and second highest MDT root priority on the FabricPath Spine switches • **Anycast HSRP**: this is recommended to provide up to four active default gateways (active-active HSRP) on the network to achieve increased high-availability. This is recommended if you are using 3-4 Spine switches or Border switches that will be connected to a Layer-3 network to provide access to other network solutions (e.g. WAN, Internet, LAN, Traditional DC) for the Spine-Leaf CLOS. • **VPC+:** this is recommended to provide active/active HSRP forwarding including creating a virtual switch that exist behind the VPC+ peers. This is recommended if you are using two Spine or Border switches that will be connected to a Layer-3 network to provide access to other network solutions (e.g. WAN, Internet, LAN, Traditional DC) for the Spine-Leaf CLOS.

Optional	• **Traffic Engineering**: provides the capability to statically configure routes into the forwarding table to specific how traffic should be routed (paths and/or interfaces) across the FabricPath domain. This operates similar to MPLS Traffic Engineering. • **EvPC+:** if you require extending VPC+ services down to Ethernet switches that are connected off of the Leaf switches in a Spine-Leaf CLOS topology. This will require adding VPC+ to the design.

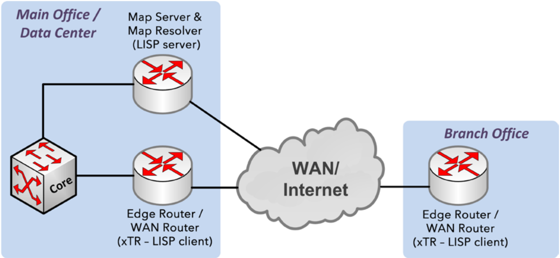
3.6.2 LISP

Select one (or more) of the following LISP PODs that will be used in the design:

	Deployment in WAN/Internet POD		

Deployment in WAN/Internet POD

POD: OVR-LISP-WAN


Main Office / Data Center
Map Server & Map Resolver (LISP server)
Core
Edge Router / WAN Router (xTR – LISP client)
WAN/ Internet
Branch Office
Edge Router / WAN Router (xTR – LISP client)

- **When to use**: this is the standard deployment for LISP configured over the WAN (or Internet)
- **Prerequisites**: WAN (or INET)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: LISP server (map server, map resolver), LISP client (ITR + ETR = xTR)
- **Description**: in this POD, the WAN routers operate as a LISP xTR which is comprised of both ITR and ETR functions. They would connect to the LISP server component for resolving and connecting with other sites. An additional router, called the LISP server, is required in the topology which will act as the LISP map server and map resolver. It would be plugged into the WAN/Internet to allow communication with the xTR enabled routers.

Configuration

Below are required, recommended, and optional configuration when deploying LISP services:

Required	• **Hardware**: it requires using Cisco router hardware that support LISP • **LISP Map Server & Resolver**: an additional router is added to the WAN to allow communication with the LISP routers. The map server is responsible for building EID-to-RLOC mappings received from the LISP client routers (ETR role) which is responsible for registering its EID prefixes with the map server. The map resolver act as the DNS server in the environment which deals with handling queries from the LISP client routers (ITR role) for resolving EID-to-RLOC requests. • **WAN Routers as LISP Clients (xTR):** this would be the WAN routers (or Internet edge routers) connected to the WAN. They would operate as a LISP xTR which is comprised of both ITR and ETR functions. The LISP client components would connect to the LISP server component for resolving and connecting with other sites.

Recommended	• **GET VPN over LISP**: LISP does not provide data encryption, only data encapsulation. It is recommended to deploy LISP as the framework between all sites. GET VPN would be built on-top of the LISP topology providing tunnel-less encryption between sites. This will require adding GET VPN to the design.

Optional	• **OTV and LISP**: OTV can be implemented with LISP to provide a “robust shortest routing path” method for extending VLANs between Data Centers. This will require adding OTV to the design. • **Virtualization**: the EID and RLOC namespaces can be virtualized within a larger LISP topology

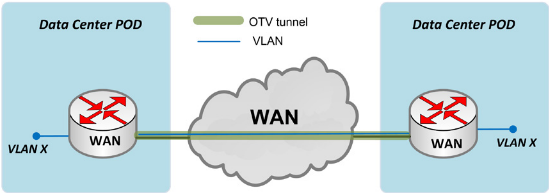
3.6.3 OTV

Select one (or more) of the following OTV PODs that will be used in the design:

	Deployment in WAN POD		

Deployment in WAN POD

POD: OVR-OTV-WAN



- **When to use**: this is the standard deployment for OTV configured over a L3WAN
- **Prerequisites**: DC, WAN-S-L3WAN (or WAN-D-L3WAN*)
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: OTV Edge (WAN router)
- **Description**: in this POD, all of the DC networks will have WAN routers connected into a L3WAN cloud. The WAN routers in this topology are configured as OTV edge devices to extend VLANs over the IP enabled WAN (L3WAN) with other Data Center networks as shown in the picture above.

Configuration

Below are required, recommended, and optional configuration when deploying OTV services:

Required

- **Hardware**: it requires using Cisco hardware that support OTV
- **Positioning**: determine where OTV will be implemented in the topology. Those devices will be configured as OTV edge devices. It will be the WAN router/switch that is connected into a L3WAN to build a connection with OTV edge devices in other Data Centers.
- Configure the overlay virtual interface referencing the WAN facing interface
- Setup the OTV site VLAN
- Define the VLANs that should be extended over the L3WAN cloud
- **OTV using Multicast**: IGMPv3 and Multicast services are required on each OTV device and across the WAN provider network

Recommended

- Do not use a user/server subnet for the OTV site VLAN. It should be its own dedicated VLAN.
- If multiple OTV edge devices (multi-homing capabilities) exist within the Data Center and will be connected to the L3WAN, Authoritative Edge Device (AED) should be enabled to avoid end-to-end loops by not sending STP BPDU messages
- **MTU Considerations**: using OTV tunneling will introduce additional overhead between the two Data Centers. It is recommended to implement either (1) Path MTU Discovery (PMTU) to dynamically discover the smallest MTU size to use to avoid fragmentation and optimize application performance over tunneled topologies. Or (2) use Jumbo Frames if supported over the L3 WAN.

Optional

- **OTV and LISP**: OTV can be implemented with LISP to provide a “robust shortest routing path” method for extending VLANs between Data Centers. This will require adding LISP to the design.

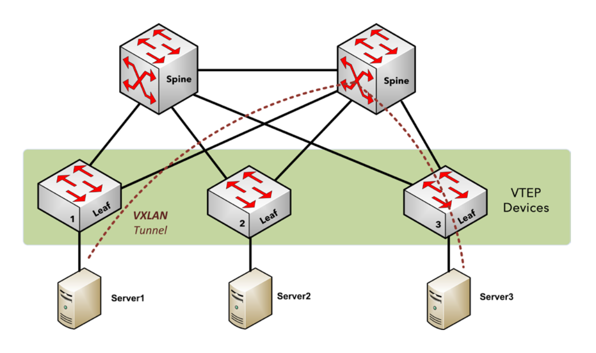
3.6.4 VXLAN

Select one (or more) of the following VXLAN PODs that will be used in the design:

	Deployment in Spine-Leaf CLOS		

Deployment in Spine-Leaf CLOS

POD: OVR-VXLAN-CLOS



- **When to use**: this is the standard deployment for VXLAN configured in a Spine-Leaf CLOS enabled Data Center
- **Prerequisites**: DC-CLOS
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: VTEP (DC Leaf/Access)
- **Description**: in this POD, the leaf switches in a Spine-Leaf CLOS are configured as VTEP devices as shown in the picture above. VXLAN runs over IP and is more scalable compared to VLANs supporting up to 16 million unique identifiers.

Configuration

Below are required, recommended, and optional configuration when deploying VXLAN services:

Required

- **Hardware**: it requires using Cisco Nexus 9000 series hardware that support VXLAN
- **Positioning**: determine where VXLAN will be implemented in the topology. Those devices will be configured as VXLAN Tunnel Endpoints (or VTEPs). It will be the Data Center leaf switches in the Spine-Leaf CLOS that will build VXLAN tunnels with other VTEPs to extend VXLANs between the virtual systems across the Data Center

Recommended

- It is recommended to use one VXLAN segment mapped to a single IP multicast group to provide optimal multicast forwarding

Optional

- **VXLAN Gateway**: connects VXLAN and VLAN segments as one forwarding domain across the Layer-3 network. It can be enabled on a VTEP device to combine a VXLAN segment and a classic VLAN segment into one common Layer-2 domain. A Cisco Nexus 9000 series switch can function as a hardware-based VXLAN gateway (and VTEP device) providing encapsulation and de-encapsulation with line-rate performance for all frame sizes.
- **Alternative to VXLAN**: VMware has a proprietary technology equivalent to VXLAN called MAC-in-MAC encapsulation. It is deployed with vCloud Director called vCloud Director Network Isolation (vCDNI) which uses MAC-in-MAC encapsulation. NVGRE is another alternative which uses GRE to tunnel Layer-2 packets over a Layer-3 network.

3.7 Quality of Service

Select one (or more) of the following QoS PODs that will be used in the design:

	QoS Traffic Classes	**QoS Deployment**	

QoS Traffic Classes
POD: QOS-CLASS
• **When to use**: this is required to determine what type of traffic should be prioritized across the network • **Prerequisites**: QOS • **Required**: -- • **Has Sub-PODs**: Go to 3.7.1

QoS Deployment
POD: QOS-DEPLOY
• **When to use**: this is required for deploying QoS services based on existing solutions such as the LAN, WAN, and VPN • **Prerequisites**: QOS-CLASS • **Required**: ATT-CON • **Has Sub-PODs**: Go to 3.7.2

3.7.1 QoS Traffic Classes

The chart below reflects a summarized view for creating QoS classifications:

Traffic Classes		Classes	DSCP	% Allocation for QoS Policies
Network Control	Diamond	1	CS6	5%
Voice	Platinum	1	EF CS3 / AF31	27 – 38%
Video		1	AF31 - 33	15%
Data	Gold Silver	1-6	AF21 – 23 AF11 - 13	17 – 32% (with Video class) 32 – 47% (without Video class)
Default / Data	Bronze	1	0	25%

- **Traffic Classes**: this column shows the type of traffic that may exist on the network. QoS is usually implemented when voice/video services will be used. The traffic classes will also be organized based on a medal tier system to show the level of priority across the network.
- **Classes**: based on the traffic class, this column reflects the number of classes/sub-classes that can be used. Among the traffic classes that is listed, the Data Class can support up to 6 sub-classes which could be Critical Data, Bulk Data, Transactional Data, etc.
- **DSCP**: based on the traffic class, this column reflects the recommended DSCP values to use for classifying and marking that type of traffic across the network. The Data class has a large range of DSCP values since it supports up to 6 sub-classes.
- **Percent Allocation**: based on the traffic class, this column reflects the bandwidth percentage you can configure in a QoS policy for LLQ and CBWFQ.

Determine what QoS classifications is needed for the network.

The examples below show how you can use the chart above for building the QoS classification that is needed in the environment:

Example #1: let’s say that our network will consist of Voice and Data traffic. For Data, we can either use the default class if we don’t have any special requirements to prioritize data traffic. Or we can use special classes (up to 6) to prioritize data traffic in our environment. Let’s say that we do not have any special requirements for classifying our data traffic. Network Control is required, so we will include that with our classification.

The percentage range for the voice class is between 27 and 38%, which will vary based on the number of concurrent calls over the WAN. If the number of calls is low, we can consider a lower number in that range. If the number is higher, we can consider the higher number. Let’s choose the higher number in that range. Therefore, the total % allocation for all classes would be: 5% + 38% + 25% = 68%

The following shows what we can use with our QoS policies:

Traffic Types	Medal Tier	Classes	DSCP	% Allocation for QoS Policies
Network Control	Diamond	1	CS6	5%
Voice	Platinum	1	EF CS3 / AF31	38%
Default / Data	Bronze	1	0	25%

Note: these allocations would only take effect if there is congestion.

With that information, we could implement a configuration like the following on a WAN router:

```
class-map match-all voice-rtp
  match ip dscp ef

class-map match-any voice-control
  match ip dscp cs3
  match ip dscp af31
```

```
policy-map WAN-POL
  class voice-rtp
  priority percent 33
class voice-control
  bandwidth percent 5
class class-default
  bandwidth percent 25
  random-detect dscp-based
```

Example #2: let's do another example. Again, let's say that our network will consist of Voice and Data traffic types. However, this time we do want to prioritize the data traffic in our environment. Network Control is required, so we will include that with our classification for reference. The percentage for the voice class will continue to use the high number. For the Data class, since we are not using a Video class, the percent range would be between 32% and 47%. Here is what we have so far:

Traffic Types	Medal Tier	Classes	DSCP	% Allocation for QoS Policies
Network Control	Diamond	1	CS6	5%
Voice	Platinum	1	EF CS3 / AF31	38%
Data	Gold Silver	1-6	AF21 – 23 AF11 - 13	32 – 47% (without Video class)
Default / Data	Bronze	1	0	25%

To determine the percentage we can use for the Data class, you can calculate the other percentages first. That would be 5% + 38% + 25% = 68%.

This means 32% (100% - 68%) would be left for the Data classes. That percentage falls within the allocated range we see in the chart. We can get a higher percentage if we lower the voice class percentage. Next, we need to determine the number of Data classes (up to 6) we want to use. Let's say we will use two sub-classes: Exchange servers (marked using AF21) and Other servers (marked using AF11). Between those two sub-classes, we need to divide the 32% between them. Therefore, we will define 17% for "Exchange Servers" and 15% for "Other Servers". Finally, below reflects what we can use with our QoS policies:

Traffic Types	Medal Tier	Classes	DSCP	% Allocation for QoS Policies
Network Control	Diamond	1	CS6	5%
Voice	Platinum	1	EF CS3 / AF31	38%
Data	Gold Silver	1-6	AF21 – 23 AF11 - 13	32% Class 1: Exchange Servers = 17% Class 2: Other Servers = 15%
Default / Data	Bronze	1	0	25%

With that information, we could implement a configuration like the following on a WAN router:

```
ip access-list standard Servers_Exchange
  permit ip 172.17.201.0 0.0.0.255

ip access-list standard Servers_Other
  permit ip 172.17.202.0 0.0.0.255

class-map match-all voice-rtp
  match ip dscp ef

class-map match-any voice-control
  match ip dscp cs3
  match ip dscp af31

class-map match-any Servers_Exchange
  match ip dscp af21
  match access-group Servers_Exchange

class-map match-any Servers_Other
  match ip dscp af11
  match access-group Servers_Other

class-map match-any network-control
  match ip dscp cs6
```

```
policy-map WAN-POL
  class voice-rtp
  priority percent 33
class voice-control
  bandwidth percent 5
class Servers_Exchange
  bandwidth percent 17
  random-detect dscp-based
class Servers_Other
  bandwidth percent 15
  random-detect dscp-based
class network-control
  bandwidth percent 5
class class-default
  bandwidth percent 25
  random-detect dscp-based
```

Templates

Below are QoS templates that can be used for QoS Classifications:

Templates	**Medal Tier Classes** Diamond Class: Network Control Platinum Class: Voice / Video Gold Class: Data - Servers Silver Class: Data - Users Bronze Class: Default/Data - Guests	

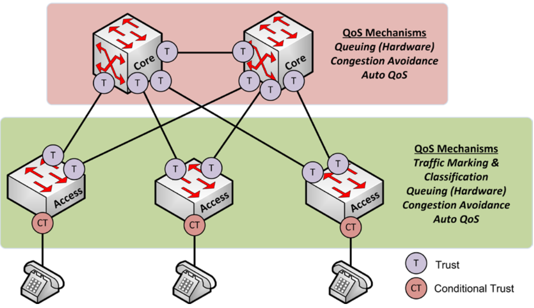
3.7.2 QoS Deployment

Select one (or more) of the following QoS deployment PODs that will be used in the design:

	Deployment in LAN POD	**Deployment in WAN POD**	**Deployment in VPN POD**

Deployment in LAN POD

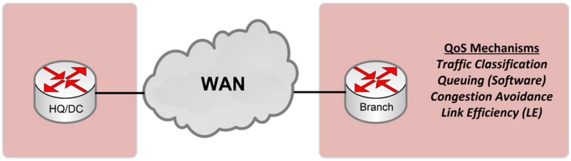
POD: QOS-LAN



- **When to use**: if the network consists of a LAN that will be deployed with QoS services
- **Prerequisites**: LAN
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: LAN Core Switch, LAN Access Switch
- **Description**: in this POD, the LAN switches are configured for trust boundaries, traffic classification, traffic markings, hardware queuing, and hardware dropping.

Deployment in WAN POD

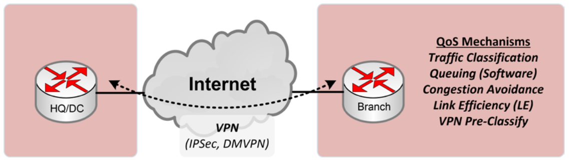
POD: QOS-WAN



- **When to use**: if the network consists of a WAN that will be deployed with QoS services
- **Prerequisites**: WAN
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: WAN routers
- **Description**: in this POD, the WAN routers are configured for traffic classification (and marking if required), software queuing, software dropping, and link efficiency mechanisms based on the WAN link of the routers.

Deployment in VPN POD

POD: QOS-VPN



- **When to use**: if the network consists of Site-to-Site VPN tunnels that will be deployed with QoS services.
- **Prerequisites**: SEC-NET-VPN-SVPN, QOS-WAN
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: VPN Routers
- **Description**: in this POD, the VPN routers will utilize the WAN POD for QoS deployment including unique link efficiency mechanisms used for VPN tunnels.

Configuration

Below are required, recommended, and optional configuration when deploying QoS services:

Required

- **QoS Traffic Classes**: it is required to determine the QoS classes that will be used based on the traffic classes determined in the QoS Classification POD

<u>Deployment in LAN POD</u>:

- **Trust Boundaries**: it is required/recommended to establish trust boundaries within the LAN POD. All uplink/downlink interfaces across the LAN should be configured as ***Trusted ports*** to trust the markings made by the IP phones and other defined endpoints. ***Conditional Trust ports*** should be enabled on all switch ports with connected IP phones and endpoints attached. All other ports by default will be treated as ***Untrusted ports***. You can also manually configure all other switch ports as Untrusted port types to avoid users/servers explicitly marking packets with high priority, which should be dedicated for real-time applications such as voice and video. It is recommended to use AutoQoS for applying the Trust boundaries (if supported).
- **QoS Marking**: based on the QoS traffic classes, determine how the traffic will be marked in the LAN POD. For voice traffic, all IP Phones in the topology will automatically mark voice packets by default according to the DSCP and COS values for voice traffic. For data traffic that will marked, this can be done on the LAN Core (based on DSCP values) or on the LAN access switches (based on CoS values) using Access Control Lists (ACL). The ACL will list the network details and will mark traffic based on the desired DSCP/CoS values. As a best practice, it is recommended to mark packets closer to the source such as the LAN Access switches with connected IP phones and endpoints.
- **QoS Classification**: in the LAN POD, all traffic will be classified based on CoS values (on Layer-2 switches) and/or DSCP values (on Layer-3 switches and Routers).

<u>Deployment in WAN POD:</u>

- **Link Speed**: determine the WAN connection and link speed for all WAN facing interfaces on the WAN routers in the topology. This will be important to understand what additional QoS mechanisms are required.
- **QoS Marking**: all traffic should already be previously marked from the LAN. Otherwise, traffic should be classified and marked on the WAN router's LAN facing interface based on the QoS traffic classes previously defined. Voice and Data traffic can be marked using Access Control Lists (ACL) or NBAR. The ACL/NBAR will list the network details and will mark traffic based on DSCP values.
- **QoS Classification**: all traffic should be classified on the WAN router's WAN facing interface based on the DSCP values and QoS traffic classes.

Recommended (1/2)

<u>Deployment in LAN POD:</u>

- **AutoQoS**: a QoS mechanism supported on Cisco switches that applies best practices of trust boundaries, queuing, and dropping. It is recommended to use option “***AutoQoS Cisco Phone***” on switch ports with connected IP Phones and endpoints. And the option “***AutoQoS Trust***” on all uplink and downlink ports across the LAN.
- **Congestion Management (Hardware Queuing):** it is recommended to use the ***Strict Priority Queue (or Expedite Queue)*** for voice and video traffic classes. And use ***Normal Queues (or WRR Queue)*** for the data, network control, and default traffic classes. Queuing is enforced when congestion occurs on a switch port.
- **Congestion Avoidance (Hardware Dropping):** it is recommended to use ***WRED*** for the data and default traffic classes to prevent congestion or queues filling up. WRED deals with gracefully dropping low priority packets before congestion occurs on a port. This is used on traffic classes with TCP type traffic because TCP has mechanisms for doing retransmissions if data packets are dropped due to congestion or loss. Implementing WRED can also increase overall throughput of TCP traffic flows.

<u>Deployment in WAN POD:</u>

- **Traffic Shaping**: this is recommended to be implemented on the WAN facing interface of the router to match the bandwidth rate of the WAN connection. But, it could affect the delay over the link.
- **Congestion Management (Software Queuing):** it is recommended to use ***LLQ*** for voice and video traffic classes. And use ***CBWFQ*** for the data, network control, and default traffic classes. Queuing is enforced when congestion occurs on an interface.
- **Congestion Avoidance (Software Dropping):** it is recommended to use ***WRED*** for the data and default traffic classes to prevent congestion or queues filling up. WRED deals with gracefully dropping low priority packets before congestion occurs on a port. This is used on traffic classes with TCP type traffic because TCP has mechanisms for doing retransmissions if data packets are dropped due to congestion or loss. Implementing WRED can also increase overall throughput of TCP traffic flows.
- **Maximum Reserve Bandwidth:** by default, interfaces on a Cisco device with a total bandwidth allocation cannot exceed 75% allowing 25% for network control related traffic. You can change the maximum reserve bandwidth to 100% if CBWFQ will be configured within a QoS policy.
- **Fragmentation**: this is recommended when the WAN link speed on the router is below 1Mbps. And the encapsulation is either PPP or Frame Relay. This is a QoS mechanism that will fragment or break-up large packets into smaller packets to allow smaller packets (e.g. Voice) to be transmitted to avoid high serialization delay and jitter. You can implement either Frame Relay Fragmentation (FRF.12) or Link Fragmentation Interleaving (LFI).
- **Compression**: this is recommended when the WAN link speed on the router is below 1Mbps. And the encapsulation is either PPP or Frame Relay. Compression RTP (cRTP) is used to compress Voice RTP packets to smaller sized packets.
- **TX-Ring Tuning**: this is required when using an ATM WAN connection with a link speed below 1Mbps. This will adjust the final interface output buffer (TX-ring) to optimal lengths for real-time traffic.

Recommended (2/2)

Deployment in VPN POD:

- **QoS Pre-Classify**: this is recommended to be enabled on VPN routers to classify traffic on the packet's header after encryption. This is applicable for WAN routers using ***IPsec over GRE*** or ***DMVPN*** implemented under the Tunnel interface.
- **Anti-Replay**: this is recommended to be enabled on VPN routers. This is a QoS mechanism that identifies whether a packet is being re-played by a hacker and confirm the integrity of the connection.
- **TCP MSS Tuning**: this is recommended to be enabled on VPN routers using ***IPsec VTI*** or ***DMVPN***. This is a QoS mechanism that provides tuning of the MSS for better TCP packet delivery across the VPN. It also helps against serialization delay which is the amount of time a router will put packets onto the physical media for transit. It is recommended to configure an MTU size of 1412 (or 1400) and MSS of 1360 on the Tunnel interface to avoid MTU related issues across the VPN tunnel.

Deployment in Storage POD:

- **QoS with FCoE**: this is recommended to provide lossless data for all FCoE traffic end-to-end within the Data Center. It uses the 802.1Q Priority Code Point or CoS bits in the Layer-2 header. It is recommended to put lossless FCoE traffic into its own hardware queue.
- **MTU**: it is recommended to use an MTU size of 2158 for FCoE
- **Drop Treatment**: it is recommended to enable "**no drop treatment**" with the QoS configuration for FCoE

Deployment in MPLS POD:

- **QoS with MPLS**: this is required if customer networks will mark packets locally within their network and will be sent across the MPLS. The MPLS network can be implemented for Uniform, Short Pipe, or Pipe mode depending on what QoS operation is required

Optional

Deployment in LAN POD:

- **Traffic Policing**: optional QoS feature to rate-limit a specific switch port to a certain bandwidth rate and keep the delay consistent (unlike traffic shaping). Any traffic that exceeds the configured threshold will be dropped.

3.8 Reliability

Select one (or more) of the following reliability services that will be used in the design:

	BFD	**Enhanced Object Tracking (EOT)**	**UDLD**
	First-Hop Redundancy Protocol		

BFD

POD: REL-BFD

- **When to use**: optional feature that can be enabled between two supported network devices to provide fast convergence if the connection between them goes down
- **Prerequisites**: REL
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Cisco L3-Device
- **Description**: this technology feature would be enabled between two directly connected routers. This protocol provides fast detection of failures on the network in sub-second times.

Enhanced Object Tracking (EOT)

POD: REL-EOT

- **When to use**: an optional feature that supports monitoring interfaces or routes then informing FHRP (or IP SLA) to make certain actions for re-routing
- **Prerequisites**: REL
- **Required**: REL-FHRP
- **Has Sub-PODs**: --
- **Components**: FHRP-enabled router
- **Description**: this technology feature would be enabled on a FHRP enabled router in the topology that can track reachability of a connected interface and/or a specific route.

First Hop Redundancy Protocol (FHRP)

POD: REL-FHRP

- **When to use**: if you require setting up two (or more) network devices to provide default gateway redundancy
- **Prerequisites**: REL, LAN-2T-PHY-FHRP (and/or DC-2T-PHY-FHRP, INET-DRSI (or INET-DRI, INET-DRFSI, INET-DRFI)
- **Required**: --
- **Has Sub-PODs**: Go to 3.8.1
- **Components**: FHRP-enabled router
- **Description**: this technology feature would be enabled on two (or more) FHRP-enabled devices for the networks that will provide default gateway redundancy.

UDLD

POD: REL-UDLD

- **When to use**: if you are using fiber cabling between two directly connected switches and want to protect against uni-directional failures
- **Prerequisites**: REL
- **Required**: Switches
- **Has Sub-PODs**: --
- **Components**: Switch
- **Description**: this technology feature would be enabled between two directly connected switches. UDLD Aggressive (recommended) should be configured on a per-port bases (between switches) not globally.

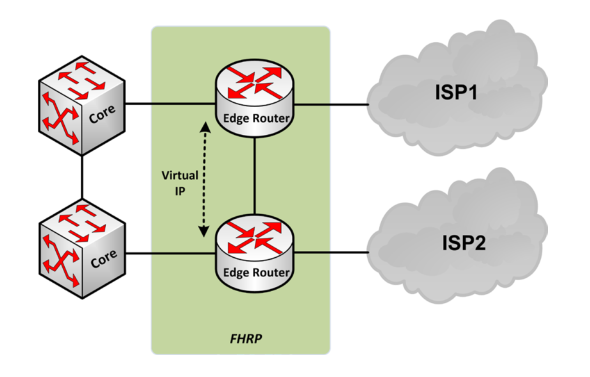
3.8.1 First-Hop Redundancy Protocol

Select one (or more) of the following FHRP PODs that will be used in the design:

	Deployment in Internet POD	**Deployment in LAN/DC POD**	

Deployment in Internet POD

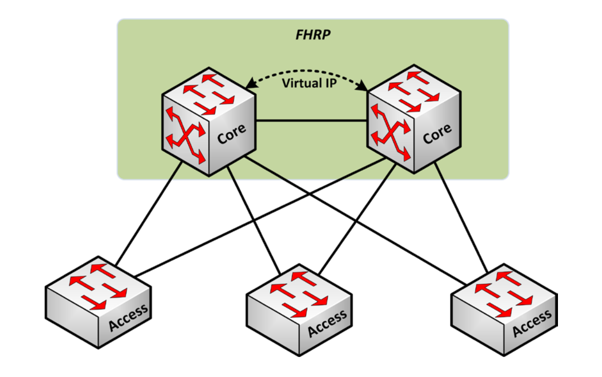
POD: REL-FHRP-INET



- **When to use**: if the network is using redundant Internet edge routers
- **Prerequisites**: INET-DRSI, DRI, DRFSI, or DRFI
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: in this POD, the two edge routers connected to one (or more) Internet clouds are configured with a FHRP (e.g. HSRP, VRRP). The Virtual IP address can be used as the default gateway for the Core switch or firewall appliance that exist behind the edge routers.

Deployment in LAN/DC POD

POD: REL-FHRP-LANDC



- **When to use**: if the network is using redundant LAN/DC Layer-3 Core switches with configured VLAN SVI (e.g. Users, Servers)
- **Prerequisites**: LAN-2T-PHY-FHRP, DC-2T-PHY-FHRP
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: in this POD, the two LAN/DC Core switches are configured with a FHRP (e.g. HSRP, VRRP) for all VLAN SVI(s) defined. The Virtual IP address is used as the default gateway for the endpoints where FHRP is enabled on that VLAN SVI.

Configuration

Select one (or more) of the following FHRP options that will be used:

	HSRP	**VRRP**	**GLBP**
	If you require setting up two (or more) network devices to provide default gateway redundancy using Cisco hardware	If you require setting up two (or more) network devices to provide default gateway redundancy	If you require setting up two (or more) network devices to provide default gateway redundancy and load-balancing

Below are required, recommended, and optional configuration when deploying FHRP services on the network based on the available options.

Required

- **Router Priority:** among the FHRP-enabled devices, determine which one will be the primary/active device and which one will be the secondary/standby network device(s).

Recommended

- **Timers**: use sub-second timers using a hello timer of 250ms and a dead timer of 750ms in environments with less than 150 VLAN instances. If those sub-second timers are not supported due to IOS/hardware limitations set the hello timer to 1 second and the dead timer to 3 seconds. This will provide a good balance of fast failover and sensitivity for traffic being sent to the control plane.
- **Tracking**: it is strongly recommended to enable tracking on the high critical interfaces (uplinks) for robust failover between FHRP peers. This is common when implementing FHRP on Internet edge routers. The WAN facing interface would be tracked. If the WAN facing interface fails on the primary FHRP device, the secondary FHRP device will take over.
- **FHRP on Cisco Catalyst Switches**: it is recommended to enable HSRP which is SSO aware which will help to avoid HSRP flapping.
- **GLBP in Redundant Three-Tier LAN Topology**: it is recommended that "spanning-tree cost 2000” be implemented on the Secondary STP root bridge switch (LAN distribution) to ensure that both uplinks from the Layer-2 switches are active.
- **HSRP and Multicast**: if Multicast and HSRP will be configured on the same device, force all data communication to use the same path. The HSRP active router should be the Designated Router (DR) on the segment.

Optional

- **Enhanced Object Tracking (EOT):** an optional feature that deals with monitoring interfaces or routes then informing FHRP (or IP SLA) to make certain actions for re-routing.

3.9 Routing

Select one (or more) of the following routing services that will be used in the design:

	OSPF	**EIGRP**	**IS-IS**
	BGP	**Static**	**Policy Based Routing (PBR)**
	IP SLA	**IP CEF**	

OSPF
POD: RT-OSPF
• **When to use**: if your internal network will have 3+ network devices capable of routing • **Prerequisites**: RT • **Required**: Routers/L3-Switches • **Has Sub-PODs**: Go to 3.9.1 • **Description**: OSPF is a IGP internal routing protocol that is configured within the LAN, Data Center, and sites across the WAN. It can provide dynamic routing with multiple Cisco/non-Cisco L3 devices on the network.

EIGRP
POD: RT-EIGRP
• **When to use**: if your internal network will have 3+ network devices capable of routing and you will have all Cisco-based hardware • **Prerequisites**: RT • **Required**: Routers/L3-Switches • **Has Sub-PODs**: Go to 3.9.2 • **Description**: EIGRP is a IGP internal routing protocol that is configured within the LAN, Data Center, and sites across the WAN. It can provide dynamic routing with multiple Cisco routing devices on the network.

IS-IS
POD: RT-ISIS
• **When to use**: if your internal network will have 3+ network devices capable of routing. Plus, support for additional IS-IS extensions. • **Prerequisites**: RT • **Required**: Routers/L3-Switches • **Has Sub-PODs**: -- • **Description**: IS-IS is a IGP internal routing protocol that is often used in service provider networks. It can be implemented on the LAN, DC, and WAN.

BGP
POD: RT-BGP
• **When to use**: if you require advertising your own Public prefixes out to the Internet. And controlling routing in (and out) of your ASN. • **Prerequisites**: INET, RT • **Required**: Routers/L3-Switches • **Has Sub-PODs**: Go to 3.9.3 • **Description**: BGP is a EGP external routing protocol which is commonly used on the Internet and advertising Public address information to Internet providers.

Static

POD: RT-STATIC

- **When to use**: if your internal network will have 1-2 network devices. This is the simplest form of routing to setup for small sized networks.
- **Prerequisites**: RT
- **Required**: Routers/L3-Switches
- **Has Sub-PODs**: --
- **Description**: static routing can be used for internal routing within a LAN/DC among a small set of L3 network devices on the network. Static routes are commonly used for default static routes configured on the edge router or firewall appliance connecting to the ISP. Default static routes can also be configured on the Core switch pointing to the edge router/firewall if a dynamic IGP routing protocol is not used.

Policy Based Routing (PBR)

POD: RT-PBR

- **When to use**: if you have unique requirements to make routing decisions based on the type of traffic and which interface it should be routed across
- **Prerequisites**: RT
- **Required**: Routers/L3-Switches
- **Has Sub-PODs**: --
- **Description**: This is used for unique routing requirements not easily accomplished through static or dynamic routing protocols. You can route packets based on the IP address/subnet (source and/or destination), application, protocol, QoS markings, to even the packet size. In most environments PBR is not needed and should be avoided to keep the routing environment simplified.

IP SLA

POD: RT-SLA

- **When to use**: an optional feature that allows re-routing/failover between connections based on pre-configured probes (or availability).
- **Prerequisites**: INET-SRDI, INET-SRFDI, or WAN-SRDW
- **Required**: Routers
- **Has Sub-PODs**: --
- **Description**: IP SLA is typically configured on routers with dual Internet connections for redundancy. IP SLA can be configured to ping a certain IP address that is specified. If the IP address is not reachable through the primary Internet connection, it will change the default route towards the secondary ISP.

IP CEF

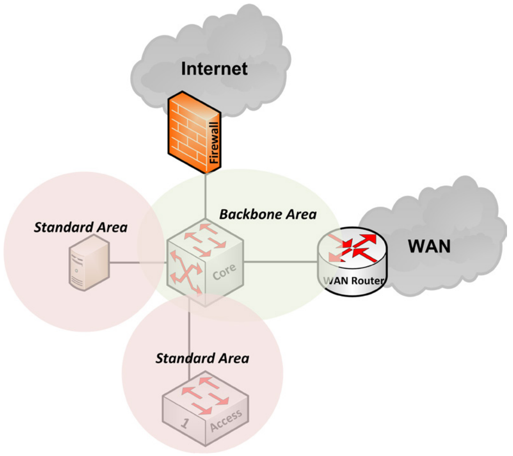
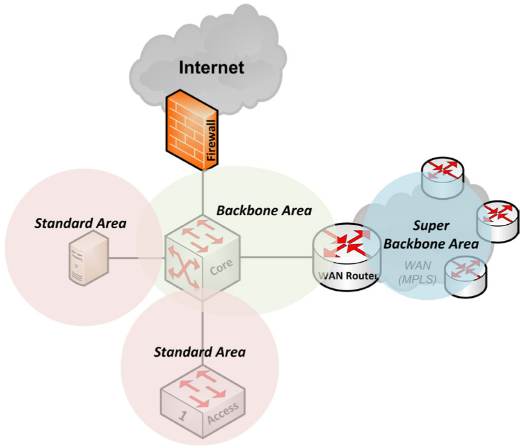
POD: RT-CEF

- **When to use**: if the LAN/DC topology has multiple paths and interconnections, it is recommended to implement CEF to provide ECMP.
- **Prerequisites**: RT
- **Required**: Cisco switches
- **Has Sub-PODs**: --
- **Description**: it is recommended to enable full IP CEF load-sharing using the L3/L4 hash algorithm to prevent CEF polarization. CEF polarization occurs when redundant paths are ignored for traffic forwarding. CEF will be able to load balance up to 8 parallel paths.

3.9.1 OSPF

Select one of the following OSPF PODs that will be used in the design:

	Standard Deployment	**Deployment with Super Backbone**	

Standard Deployment	Deployment with Super Backbone
POD: RT-OSPF-STD	**POD**: RT-OSPF-MPLS
 Internet Firewall Backbone Area Standard Area Core WAN WAN Router Standard Area 1 Access	 Internet Firewall Backbone Area Standard Area Core WAN Router Super Backbone Area WAN (MPLS) Standard Area 1 Access
• **When to use**: this is a standard deployment for OSPF configured within the LAN, DC, and/or WAN (not using MPLS) • **Prerequisites**: LAN and/or DC • **Required**: -- • **Has Sub-PODs**: -- • **Components**: OSPF routers • **Description**: in this POD, the network consist of a backbone area with several standard areas connected as shown in the picture above. Using areas will break up the network into multiple flooding domains. This is a standard deployment if you not using a MPLS-enabled L3WAN in the environment.	• **When to use**: if you require extending OSPF over a L3WAN managed by a service provider • **Prerequisites**: LAN/DC, WAN-S-L3WAN (or WAN-D-L3WAN*) • **Required**: -- • **Has Sub-PODs**: -- • **Components**: OSPF routers • **Description**: in this POD, the network consist of a backbone area with several standard areas connected. Using areas will break up the network into multiple flooding domains. The backbone area would be extended over the MPLS-enabled L3WAN and would be a Super Backbone area as shown in the picture above. The remote sites would connect to the Super Backbone area along with standard areas connected internally.

Configuration

Below are required, recommended, and optional configuration when deploying OSPF services:

Required

- **Backbone Area**: this is required for all OSPF networks. This area is typically deployed among the Core, Distribution, and WAN routers in the topology.
- **Standard Areas**: determine the standard areas that will be connected to the Backbone area. These areas will be LAN/DC Layer-3 access switch networks, endpoint networks (e.g. User, Server), and network solutions (e.g. Internet, Firewall). All routers that connect between the backbone area and a standard area will be considered as an Area Border Router (ABR).
- **Advertised Networks**: determine the networks on each router that should be advertised among the OSPF routers. This would be networks that are configured on interfaces (physical or SVI interfaces) that are connected into the OSPF domain. This would involve adding that network and its associated area under the OSPF routing process.

Recommended (1/2)

- You should have no more than 50 routers within a single area
- You should have no more than 60 neighbors established on a OSPF router
- ABRs should have up to 3 areas attached
- **Passive Interfaces**: it is recommended to enable passive interfaces to prevent rogue routing devices from injecting bad routes into the network. It should be enabled on all Layer-3 interfaces where there are endpoints and no OSPF routers present on that segment. This will prevent hello messages being sent and establishing any adjacencies with other OSPF routers.
- **Route Authentication**: it is recommended to configure MD5 Authentication on all OSPF routers to provide higher security compared to implementing Passive Interfaces only. The password defined will be required to form a neighbor relationship with other OSPF routers on the network. OSPFv3 uses IPsec for route authentication in a IPv6 enabled network.
- **Hello and Dead Timers**: it is recommended to tune the OSPF timers to provide fast convergence if a failure occurs. This can be accomplished by adjusting the default hello and dead timers. You can tune the timers to smaller values like 1 second for the hello and 4 seconds for the dead timer. Furthermore, OSPF in later OS versions can provide fast timers in sub-second intervals.
- **Route Summarization**: it is recommended to summarize multiple routes as a single route to help minimize the size of the routing table, reduce hardware resources (CPU, memory), and to limit LSA flooding. It can also help to provide fast convergence from failures that may occur on the Layer-3 network. This can be implemented in several ways depending on the overall topology: (1) it can be implemented on the distribution switches in a Tier-3 topology. It can summarize the user subnets which would be advertised to the Core and other OSPF routers. (2) It can implemented on the Core if there are several networks that can be summarized. This summarized route would be advertised to other network devices (e.g. WAN routers, Internet router/firewall). (3) It can be implemented on the WAN aggregation routers. It can summarize the remote site subnets which would be advertised to the Core (and other OSPF devices).
- **IP CEF**: it is recommended to implement CEF switching on all OSPF enabled devices to provide fast convergence and ECMP (if there are multiple paths available).
- **Loopback Interfaces**: it is recommended to use Loopback interfaces on all OSPF routers (IPv4 and IPv6) in the topology which will be used as the router-ID for the OSPF router
- **Stub or Totally Stub Areas**: it is recommended to enable OSPF stub areas for the WAN remote sites and LAN Access networks enabled for Layer-3 services (if applicable). This will help to minimize the size of the routing table and to limit LSA flooding within an area. This includes preventing unnecessary SPF calculations that may occur.
- **Route Control/Filtering**: it is recommended to control what routes are being sent and received between OSPF routers using a distribute list (or route-map). This is commonly deployed with OSPF routers that are managed by a different building/group.
- **Network Type using Point-to-Point Network**: this network type is recommended for point-to-point connections between two OSPF devices.

Recommended (2/2)

- **Network Type using Broadcast Network**: this is the default network type for Ethernet networks. This is recommended for full-mesh networks used on the WAN or OSPF routers connected in the same VLAN. A DR and BDR are elected to reduce LSA flooding within the area. It is recommended for the Core (or distribution switch) to be the DR for those segments.
- **Equal Cost Path (ECP):** multiple connections on the LAN/DC can provide fast convergence and load balancing of traffic through the network. This is accomplished by creating multiple paths using the same metric value (cost), which will inject two (or more) paths for a destination into the global routing table.
- **IPv6 OSPF**: OSPF has support for IPv6 which would be implemented directly on the IPv6 enabled interfaces. This will (1) add the IPv6 network automatically under the routing process and (2) be used for neighbor discovery.

Optional

- Use **Virtual links** if there are two standard areas connected together
- Enable **LSA Throttling** in large-scale networks with hundreds of routers to provide fast convergence within the OSPF topology. This will provide LSA rate-limiting in milliseconds compared to seconds. This is enabled by default, but it can be tuned to control LSA flooding more efficiently when there is a topology change.
- Enable **SPF Throttling** in large-scale networks with hundreds of routers to provide fast convergence for SPF calculations in millisecond intervals when there is a topology change. The default behavior is based on dynamic calculations, but it’s recommended to tune these values in larger OSPF environments.
- Enable **Incremental SPF (iSPF)** in large-scale networks with hundreds of OSPF routers to provide SPF optimization and fast convergence. This will allow OSPF routers to recalculate only the affected parts of the topology and not waste router resources (CPU).
- **BFD with OSPF**: BFD can be configured in conjunction with OSPF to provide faster convergence if there is an interface failure.
- **Primary and Secondary Paths**: if you have dual connections within the WAN or Internet POD, you can designate a primary and secondary path by adjusting the OSPF cost. For example, the primary path interface can be configured with a cost of 10. And the secondary path interface can be configured with a cost of 1000. As a result, the primary path would be preferred instead of the secondary path.
- **Route Redistribution:** if you require integrating a different routing domain (e.g. EIGRP) with the existing network running OSPF. Route Redistribution must be configured between the two routing protocols. It is important to implement route filtering to control what routes should be advertised and received between the two routing domains.

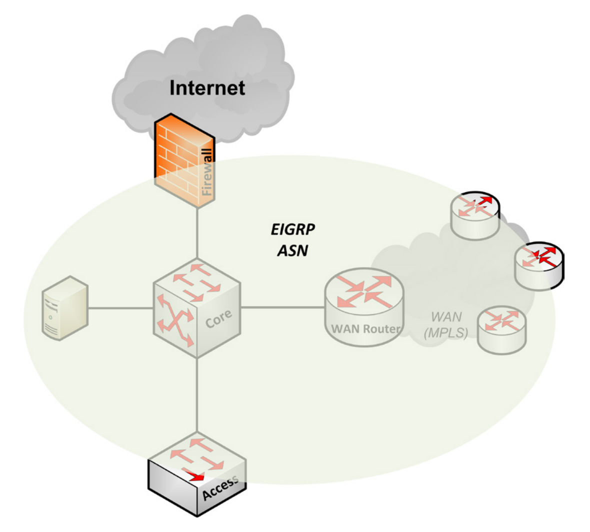
3.9.2 EIGRP

Select one of the following EIGRP PODs that will be used in the design:

	Standard Deployment		

Standard Deployment

POD: RT-EIGRP-STD



- **When to use**: this is a standard deployment for EIGRP configured within the LAN, DC, and/or WAN
- **Prerequisites**: LAN/DC
- **Has Sub-PODs**: --
- **Components**: EIGRP routers
- **Description**: in this POD, all of the Cisco Layer-3 devices are configured for EIGRP under the same ASN as shown in the picture above. Each network configured on the device would be added to the routing process (using IPv4) or interface (using IPv6) to be exchanged with other EIGRP routers.

Configuration

Below are required, recommended, and optional configuration when deploying EIGRP services:

Required

- **ASN**: determine the Autonomous System Network (ASN) each EIGRP router will belong to for exchanging route information. If an EIGRP router is not in the same ASN with other EIGRP routers it will not be able to build a neighbor or exchange routes with other routers in the AS.
- **Advertised Networks**: determine the networks on each router that should be advertised among the EIGRP routers. This would be networks that are configured on interfaces (physical or SVI interfaces) that are connected into the EIGRP AS. This would involve adding that network under the EIGRP routing process.

Recommended

- **Passive Interfaces**: it is recommended to enable passive interfaces to prevent rogue routing devices from injecting bad routes into the network. It should be enabled on all Layer-3 interfaces where there are endpoints and no EIGRP routers present on that segment. This will prevent hello messages being sent and establishing any adjacencies with other EIGRP routers.
- **Route Authentication**: it is recommended to configure MD5 Authentication on all EIGRP routers to provide higher security compared to implementing Passive Interfaces only. The password defined will be required to form a neighbor relationship with other EIGRP routers on the network.
- **Disable Auto Summarization:** EIGRP will automatically summarize networks along major network boundaries. It is recommended to disable auto-summarization and use manual summarization instead (if required).
- **Route Summarization**: it is recommended to summarize multiple routes as a single route to help minimize the size of the routing table, reduce hardware resources (CPU, memory), and to prevent unnecessary EIGRP queries. It can also help to provide fast convergence from failures that may occur on the Layer-3 network. This can be implemented in several ways depending on the overall topology: (1) it can be implemented on the distribution switches in a Tier-3 topology. It can summarize the endpoint subnets which would be advertised to the Core and other EIGRP routers. (2) It can implemented on the Core if there are several networks that can be summarized. This summarized route would be advertised to other network devices (e.g. WAN routers, Internet router/firewall). (3) It can be implemented on the WAN aggregation routers. It can summarize the remote site subnets which would be advertised to the Core (and other EIGRP devices).
- **IP CEF**: it is recommended to implement CEF switching on all EIGRP enabled devices to provide fast convergence and ECMP (if there are multiple paths available)
- **Hello and Hold Timers**: it is recommended to tune the EIGRP timers to provide fast convergence if a failure occurs. This can be accomplished by adjusting the default hello and hold timers. The hold timer is important to trigger a convergence when a failure occurs with an established neighbor. You can tune the timers to smaller values like 1 second for the hello and 3 seconds for the hold timer. Or 2 seconds for the hello and 8 seconds for the hold timer.
- **Stub Routing**: it is recommended to configure the WAN remote site routers and LAN Layer-3 Access networks (if applicable) as EIGRP stub routers. This will prevent EIGRP queries being sent to those routers and can reduce router resources. It will also prevent those routers from being a transit device for reaching other networks such as other remote sites.
- **Route Control/Filtering:** it is recommended to control what routes are being sent and received between EIGRP routers using a distribute list. This is commonly deployed with EIGRP routers that are managed by a different building/group.
- **Equal Cost Path (ECP):** multiple connections on the LAN/DC can provide fast convergence and load balancing of traffic through the network. This is accomplished by creating multiple paths using the same metric value (delay), which will inject two (or more) paths for a destination into the global routing table.
- **IPv6 EIGRP**: EIGRP has support for IPv6 which would be implemented directly on the IPv6 enabled interfaces. This will (1) add the IPv6 network automatically under the routing process and (2) be used for neighbor discovery.

Optional	• **NSF with EIGRP**: this should be enabled if the EIGRP enabled device is using a Cisco Catalyst switch with redundant supervisor modules. If the primary supervisor fails, IP traffic would continue to be forwarded in hardware and failover to the standby supervisor module. However, the supervisor needs time to re-establish two-way peering with all connected EIGRP neighbors. Enabling NSF with EIGRP can alert the connected neighbors about the switchover and allow time to re-establish all connections gracefully. • **BFD with EIGRP**: BFD can be configured in conjunction with EIGRP to provide faster convergence if there is an interface failure • **EIGRP Over the Top (OTP):** if you require using WAN routers running EIGRP over the Internet without using VPN tunnels. GET VPN can be configured with EIGRP OTP, which uses LISP, to provide encryption services. • **Primary and Secondary Paths**: if you have dual connections within the WAN or Internet POD, you can designate a primary and secondary path by adjusting the EIGRP delay. For example, the primary path interface can be configured with a delay of 10. And the secondary path interface can be configured with a delay of 1000. As a result, the primary path would be preferred instead of the secondary path. • **Route Redistribution:** if you require integrating a different routing domain (e.g. OSPF) with the existing network running EIGRP. Route Redistribution must be configured between the two routing protocols. It is important to implement route filtering to control what routes should be advertised and received between the two routing domains.

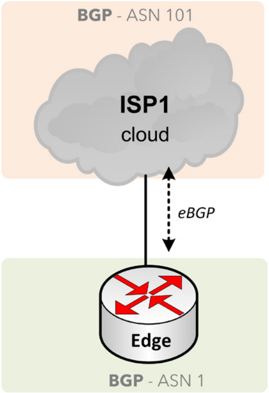
3.9.3 BGP

Select one (or more) of the following BGP PODs that will be used in the design:

	Standard Deployment	**Deployment with Weight**	**Deployment with MED**
	Deployment with Local Preference	**Deployment with AS Path Prepending**	**Deployment with Route Reflectors**

Standard Deployment

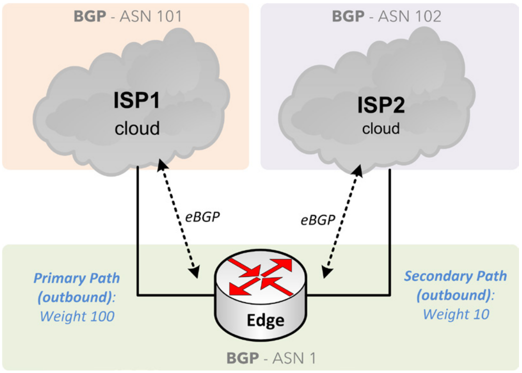
POD: RT-BGP-STD



- **When to use**: if you have a single edge router/firewall appliance that will establish a BGP connection to a single ISP
- **Prerequisites**: INET-SRI, SFI, or SRFI
- **Required**:
- **Has Sub-PODs**: --
- **Components**: Edge routers (or Firewall appliance)
- **Description**: in this POD, a single edge router (or firewall appliance) will establish a BGP connection to a single ISP. The edge router (or firewall appliance) will exist in a Public ASN that is registered for the business. No other BGP configuration such as attributes and communities is required.

Deployment with Weight

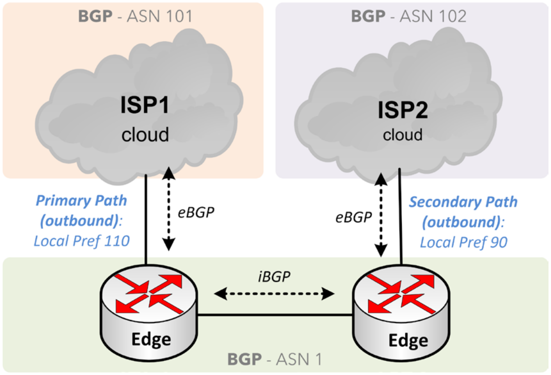
POD: RT-BGP-WT


BGP - ASN 101
ISP1
cloud
BGP - ASN 102
ISP2
cloud
eBGP
eBGP
Primary Path (outbound): Weight 100
Edge
Secondary Path (outbound): Weight 10
BGP - ASN 1

- **When to use**: if the Internet POD consists of one edge router (or firewall appliance) connected to multiple ISPs. And you want to perform primary outbound routing through a specific router/firewall/ISP.
- **Prerequisites**: INET-SRDI, SFDI, or SRFDI
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Edge router (or Firewall appliance) supporting BGP Weight
- **Description**: in this POD, a single edge router (or firewall appliance) within the Internet POD will be configured for BGP and will connect to two (or more) ISP clouds as shown in the picture above. The BGP attribute, Weight, would be implemented on each ISP link for all inbound routes received from the two ISP clouds. The primary interface would have a higher weight value compared to the secondary interface. As a result, access to the Internet would go through the primary interface. If there is an outage, Internet access would be routed through the secondary interface.

Deployment with Local Preference

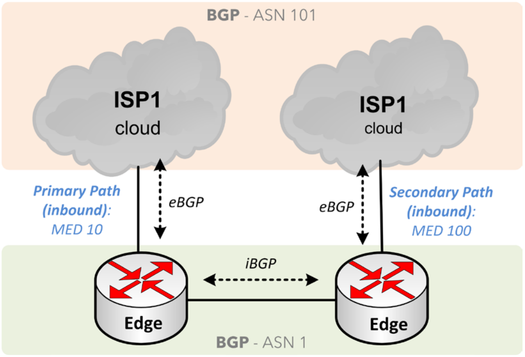
POD: RT-BGP-LP


BGP - ASN 101
ISP1
cloud
BGP - ASN 102
ISP2
cloud
Primary Path (outbound): Local Pref 110
eBGP
eBGP
Secondary Path (outbound): Local Pref 90
iBGP
Edge
Edge
BGP - ASN 1

- **When to use**: if the Internet POD consists of multiple edge routers (or firewall appliances) located in the same ASN. And you want to perform primary outbound routing through a specific router/firewall/ISP.
- **Prerequisites**: INET-DRSI, DFSI, DRI, DFI, DRFSI, or DRFI
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Edge routers (or Firewall appliances) supporting BGP Local Preference
- **Description**: in this POD, the two edge routers (or firewall appliances) within the Internet POD will be configured for BGP in the same ASN. The two BGP routers would be connected to one (or more) ISP clouds as shown in the picture above. The BGP attribute, Local Preference, would be implemented on both BGP routers for all inbound routes received from its connected ISP. The primary device/path would have a higher local preference value compared to the secondary device in the topology. As a result, access to the Internet would go through the primary device/path. If there is an outage, Internet access would be routed through the secondary device/path.

Deployment with MED

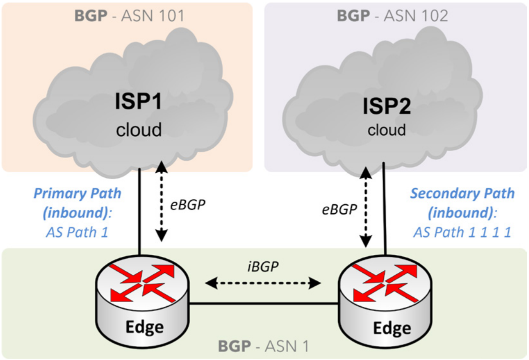
POD: RT-BGP-MED



- **When to use**: if the Internet POD consists of one (or more) edge routers (or firewall appliances) connected to multiple ISPs in the same ASN. And you want to perform primary inbound routing through a specific edge router (or firewall appliance).
- **Prerequisites**: INET-DRSI,DFSI,DRI,DFI,DRFSI, or DRFI
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Edge routers (or Firewall appliances) supporting BGP MED
- **Description**: in this POD, one (or more) edge routers (or firewall appliances) within the Internet POD will be configured for BGP in the same ASN. Both edge routers (or firewall appliances) would connect to an ISP in the same ASN. The BGP attribute, MED, would be implemented on each edge router (or firewall appliance) for all outbound routes advertised to the ISP. The primary device would advertise a low metric value compared to the secondary device in the topology. As a result, access into the customer network would be routed through the primary device. If there is an outage, inbound access would be routed through the secondary device. The MED attribute is sometimes stripped by the ISP, so it is important to confirm these details with the ISP.

Deployment with AS Path Prepending

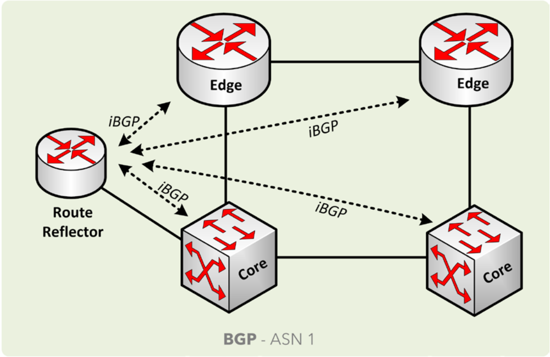
POD: RT-BGP-ASPP



- **When to use**: if your Internet POD consists of one (or more) edge routers (or firewall appliances) connected to multiple ISPs in different ASNs. And you want to perform primary inbound routing through a specific router/firewall/ISP.
- **Prerequisites**: INET-DRSI,DFSI,DRI,DFI,DRFSI, or DRFI
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Edge routers (or Firewall appliances) supporting BGP AS Path Prepending
- **Description**: in this POD, one (or more) edge routers (or firewall appliances) within the Internet POD will be configured for BGP in the same ASN. Both edge routers (or firewall appliances) would be connected to one (or more) ISP located in different ASNs. AS Path Prepending would be implemented on the secondary device for all outbound routes advertised to its connected ISP. The primary device would have the default AS path for the advertised networks. However, the secondary device would have the AS Path prepended several times creating a longer undesired path. As a result, access into the customer network would be routed through the primary device which has the shortest AS path into the network. If there is an outage, inbound access would be routed through the secondary device.

Deployment with Route Reflectors

POD: RT-BGP-RR



- **When to use**: if the internal network has 3 (or more) iBGP routers within the local ASN
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Edge routers (or Firewall appliances) supporting BGP Route Reflectors
- **Description**: if the internal routing protocol used is BGP, it is recommended to implement Route Reflectors (or Confederations) to prevent configuring a full-mesh of iBGP neighbors. In this topology, an additional routing device is added to the network (connected to the Core switch) which will act as the Route Reflector server. All iBGP routers (acting as Route Reflector clients) would peer with the server instead of being fully-meshed between each other.

Configuration

Below are required, recommended, and optional configuration when deploying BGP services:

Required

- **ASN**: determine the Autonomous System Network (ASN) each BGP router will belong to. This ASN is obtained through ARIN among other IP requirements. A private ASN can be used internally if BGP will be configured with a provider that will translate it to a Public ASN.
- **Peering (iBGP, eBGP):** determine what BGP routers will be connected as peers. The edge routers/firewall appliances in the topology (existing in the same ASN) would be considered as iBGP peers. The ISP cloud(s) would be eBGP peers (existing in a different ASN).
- **Routes Advertised**: determine what Public subnets will be advertised from your ASN
- **Routes Received**: determine what routes should be received from the ISP or EBGP peer. The ISP can either send the full routing table (requires high-end hardware with a lot of memory), a partial routing table, or just a BGP default route. A BGP default route is recommended for most customer networks which doesn't require high-end hardware. Larger networks or hosting/cloud provider networks will typically require full routes for better control of routing to certain networks.

Recommended

- **MD5 Authentication**: it is recommended to configure a password with the connected eBGP peer for establishing a neighbor and exchanging route information. This can prevent against peering with rogue BGP devices.
- **Summarization**: if you are advertising multiple Public subnets within a customer ASN, it is recommended to summarize those routes first, if possible. This will create smaller routing tables and use less hardware resources. It is a best practice to aggregate routes into longer-prefix routes on eBGP connections (e.g. ISP).
- **Soft Reconfiguration**: this is recommended to allow graceful BGP neighbor restarts when changes occurs. It should be enabled for all BGP peers to eliminate the need to reset a neighbor including the routing table in a production environment.
- **Route Control/Filtering**: it is recommended to control what routes are advertised and received from other BGP peers. This can prevent rogue BGP routers potentially bringing down the entire network. You can setup route filters using either Prefix Lists (recommended) or Distribution Lists.
- **Synchronization**: by default, routes on a BGP router that are not learned via an IGP routing protocol will not be injected into the BGP routing table. Make sure that each network you list under the BGP routing process has a matching route (dynamic, static, discard route) added.
- **iBGP using Route Reflector or Confederation**: if there are more than 3-4 iBGP routers within the ASN, it is recommended to implement Route Reflectors or a Confederation to prevent a full-mesh of iBGP neighbors. To prevent loops, route reflector client should never be peered to a route reflector through another route reflector. Furthermore, a route reflector uses a cluster ID. It is important to define the cluster ID carefully because a BGP router may reject routes if its local cluster ID is in the cluster list.
- **Fast Convergence**: you can implement ***Fast Failover*** to improve BGP convergence over a point-to-point connection compared to the default BGP timers. This will use BGP Selective Address Tracking and Fast External Neighbor Loss Detection. You can also configure ***Fast Peering Session Deactivation*** to monitor BGP peers and provide fast convergence.
- **Prefix Independent Convergence (PIC) and Add-Path**: used to provide fast sub-second convergence by creating a best path and a second best path to reach a destination network
- **Peer Groups**: all BGP neighbors that share the same identical outbound policies can be configured together into a peer group to simplify the configuration of the BGP neighbors

Optional	• **eBGP Multi-Hop**: by default EBGP peers must be directly connected (TTL of 1). If the EBGP peer is not directly connected then ***eBGP multi-hop*** must be added reflecting the number of hops to that EBGP peer (up to 255 hops). • **BGP Communities**: if you require specifying rules for how certain routes should be forwarded by BGP routers in different ASNs. • **Conditional Advertisements**: if you require BGP routers to only advertise its configured prefixes through another eBGP peer if certain routes do not exist in the BGP routing table. • **Outbound Route Filtering (ORF):** this is a feature used to filter outbound BGP route advertisements from a neighboring BGP router. • **BGP Link State (BGP-LS):** this is used to export IGP information from the network to a SDN controller to build a topology map.

3.10 Security

Select one (or more) of the following security service PODs that will be used in the design:

	General Best Practices	**Access Control List (ACL)**	**802.1X**
	Virtual Private Network (VPN)		

General Best Practices

POD: SEC2-GEN

- **When to use**: these are general best practices that should be implemented on all network devices if supported
- **Prerequisites**: SEC2
- **Required**: --
- **Has Sub-PODs**: Go to 3.10.1

Access Control List (ACL)

POD: SEC2-ACL

- **When to use**: if you will be implementing firewall services between two (or more) networks on a router and/or Layer-3 switch device
- **Prerequisites**: SEC-NET-FW-DEPLOY-INTG*
- **Required**: --
- **Has Sub-PODs**: Go to 3.10.2

Virtual Private Network (VPN)

POD: SEC2-VPN

- **When to use**: if you will be using a VPN solution within the network
- **Prerequisites**: SEC-NET-VPN
- **Required**: --
- **Has Sub-PODs**: Go to 3.10.3

802.1X

POD: SEC2-8021X

- **When to use**: if you want to authenticate users before they gain access to the network (wired or wireless)
- **Prerequisites**: LAN
- **Required**: OPS-AUTH
- **Has Sub-PODs**: Go to 3.10.4

3.10.1 General Best Practices

Below are recommended best practices to implement on the network.

Recommended (1/2)

- **RFC 1918 Addressing**: it is recommended for all internal endpoints (e.g. users, servers) to use RFC 1918 private addressing and not public addressing
- **Point-to-Point Connections**: it is recommended to use /30 subnets for all point-to-point connections. If OSPF is used, configure the network type on those interfaces to be “point-to-point”.
- **Speed and Duplex**: majority of network performance issues are related to speed and duplex mismatching between the network port and the device. It is recommended for the endpoints and its connected switch port to use auto negotiation for the speed and duplex settings.
- **VTY Access using SSH**: VTY is used for administrating a network device remotely using Telnet or SSH. It is recommended to use SSH instead of Telnet which provides a secure connection between the client and the network device for administration.
- **Proxy ARP**: disable ***proxy-arp*** services on all interfaces especially firewall interfaces which can cause performance related issues on the network
- **Unicast Reverse Path Forwarding (uRPF):** this feature is used to protect against IP spoofing attacks (not blocking DoS attacks). For each packet received on a uRPF enabled interface, it is checked against the routing table. If the source IP is not from the correct interface in which it is received, the packet will be dropped. Enable this feature on the edge router’s WAN facing interface(s). Implementing uRPF requires CEF to be enabled globally on the network device.
- **Scheduler**: configure a scheduler on the Cisco network devices to allow adequate CPU processor time to run control plane related services. This will help to prevent against fast flooding attacks that can affect critical processes from running on the device. Set the schedule interval to 500ms.
- **ACL for SNMP and NTP Services**: for tighter security it is recommended to implement ACL policies for SNMP and NTP services
- **Time Services (NTP)**: it is recommended to enable time services on all network devices in the environment. This will provide proper timestamps for logs and events that are reported. Therefore configure NTP, service timestamps, and time-zones on all network devices.
- **Unused Interfaces**: any interface that is not used on a network device should either be placed in a shutdown state or configured in a disabled VLAN.
- **Security Login Banner**: it is recommended to add a Message of the Day (MOTD) banner displaying details who is authorized to access the device. Never use words like "Welcome" in the message banner as it implies that anyone can access the device without authorization.
- **Layer-3 Interfaces**: Proxy-ARP, IP Unreachables, Directed Broadcast, and IP Mask Reply should be disabled on all Layer-3 interfaces. IP Unreachables should be disabled to prevent denied ACL traffic being leaked to the control plane (e.g. MFSC at 10pps per VLAN).
- **Disable Services**: as a general best practice the following services should be disabled globally on all network devices: TCP and UDP small services, BOOTP services, Finger, Configuration Auto-load, and PAD, HTTP services. Many of these are legacy services that are no longer used today.
- **Logging (Syslog)**: it is recommended to setup logging on all network devices for recording network events. The log messages can be stored locally or sent to a centralized Syslog server (recommended). It is also recommended to implement time services and sequence numbers with log messages to view the order of events logged.

Recommended (2/2)

- **CDP**: it is recommended to enable CDP globally on the LAN access switches with IP phones attached. However, it is recommended to disable CDP on interfaces that connect to a service provider or a network under a different administration.
- **Password Encryption**: this should be enabled globally on all network devices to provide basic password encryption in the configuration files. However, configuring MD5 passwords for increased security is strongly recommended.
- **Control Plane Protection**: the following services can be implemented to protect control plane related traffic on a network device. These services include CEF, CoPP, ACL, Broadcast Suppression, Selective Packet Discard (SPD) checks, to Hardware Rate Limiters (if supported on the hardware).
- **Data Plane Protection**: the following services can be implemented to protect the data plane where traffic is forwarded in hardware. These services include DHCP Snooping, Dynamic ARP Inspection (DAI), and IP Source Guard. These are services referenced in the Switching POD. Other services include RFC1918 filtering, RFC2728 (Anti-Spoofing) filtering, Traffic Policing, and implementing Unicast Reverse Path Forwarding (uRPF).
- **Configuration Rollback**: this is a recommended feature (if supported) that allows replacing an active running configuration with any saved configuration. This can be used to restore a previous configuration file to a network device. It can automatically save the configuration file locally or be sent to a server on the network. This feature is supported on most Cisco Catalyst and the Nexus series switches.
- **Network Monitoring & Troubleshooting:** it is recommended to implement NTP, Logging, SNMP, and NetFlow services among the network devices in the topology

Optional

- **Role-Based Access Control (RBAC):** a feature that provides restricted CLI access with different privilege levels for technicians and engineers. This will simplify administration and avoid potential misconfiguration resulting in outages.
- **NULL (Black Hole) Routing**: this is an optional security practice to configure static routes for host IP Addresses (internal or external) that should be restricted for access across the network. The next hop for these routes would be the NULL interface where packets to that IP would be discarded.
- **Out-of-Band (OOB) Management**: determine how the network devices will be accessed during network outages. This can be through a dedicated Internet connection and/or an analog connection.

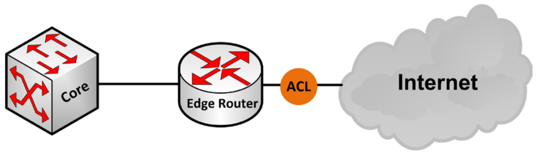
3.10.2 Access Control Lists (ACL)

Select one (or more) of the following ACL PODs that will be used in the solution:

	Deployment in Internet POD	**Deployment in LAN/DC POD**	

Deployment in Internet POD

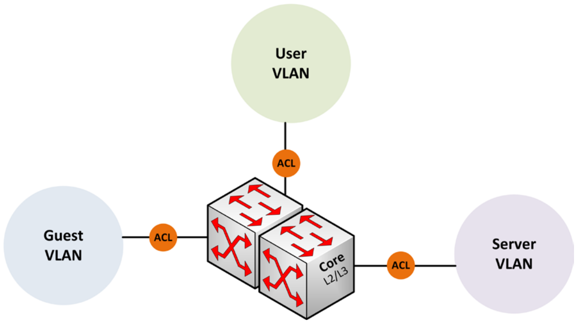
POD: SEC2-ACL-INET



- **When to use**: if ACL services will be implemented on the Internet edge router within the Internet POD
- **Prerequisites**: INET, SEC-NET-FW-DEPLOY-INTG1
- **Required**: --
- **Components**: Edge router
- **Description**: in this POD, ACL services are enabled on the Internet edge router's WAN facing interface acting as a basic Stateful firewall as shown in the picture above.

Deployment in LAN/DC POD

POD: SEC2-ACL-LANDC



- **When to use**: if ACL services will be implemented on the Core switch within the LAN and/or DC POD
- **Prerequisites**: LAN/DC, SEC-NET-FW-DEPLOY-INTG2
- **Required**: --
- **Components**: Core switch
- **Description**: in this POD, ACL services are enabled on the Layer-3 Core switches VLANs interfaces (SVI) to restrict communicate between the VLANs (e.g. User VLAN, Server VLAN, Guest VLAN) as shown in the picture above.

Configuration

Select one (or more) of the following ACL options that will be used:

	Standard / Extended ACL Provides basic security policies that are configured on an interface	**Reflexive ACL (rACL) / CBAC** Provides Stateful firewall capabilities on a Cisco IOS device	**Zone Based Firewall (ZFW)** Firewall feature that creates a Stateful firewall by creating zones on the interfaces of a Cisco IOS router

Below are required, recommended, and optional configuration when deploying ACL services on the network based on the available options.

Required	• **Positioning**: determine where ACL services will be implemented in the topology based on the firewall solution designed

Recommended	• **Stateful Firewall using rACL or CABC**: it is recommended to implement a Stateful ACL feature-set using either Reflexive ACLs or CBAC. From the two, I would recommend rACL to provide a software-based Stateful firewall on a router. I encountered some low throughput and HTTP related issues when using CBAC as a Stateful firewall, which was easily fixed when rACL was configured. • **Using Standard ACL**: if you require filtering based on the source IP address (or subnet). This should be considered if the Layer-3 device doesn't support a Stateful firewall feature-set. • **Using Extended ACL**: if you require filtering based on the destination IP address, subnet, protocol, and/or port number. This should be considered if the Layer-3 device doesn't support a Stateful firewall feature-set.

3.10.3 Virtual Private Network (VPN)

Select one (or more) of the following VPN PODs that will be used in the design:

IPsec VPN	**DMVPN**	**GET VPN**
SSL VPN		

IPsec VPN

POD: SEC2-VPN-IPSEC

- **When to use**: if you require building a point-to-point secure connection between two sites and/or to provide a remote access solution for clients
- **Prerequisites**: SEC-NET-VPN-IPSEC
- **Required**: Router or Firewall appliance
- **Has Sub-PODs**: Go to 3.10.3.1

DMVPN

POD: SEC2-VPN-DMVPN

- **When to use**: if you require building multiple VPN tunnels among routers in a hub-and-spoke topology
- **Prerequisites**: SEC-NET-VPN-DMVPN
- **Required**: Cisco Routers
- **Has Sub-PODs**: Go to 3.10.3.2

GET VPN

POD: SEC2-VPN-GETVPN

- **When to use**: if you require providing end-to-end data encryption and communication without using VPN tunnels
- **Prerequisites**: SEC-NET-VPN-GETVPN
- **Required**: Cisco routers
- **Has Sub-PODs**: Go to 3.10.3.3

SSL VPN

POD: SEC2-VPN-SSL

- **When to use**: if you require using HTTPS for your remote access (client VPN) solution
- **Prerequisites**: SEC-NET-VPN-SSL
- **Required**: Router or Firewall appliance
- **Has Sub-PODs**: Go to 3.10.3.4

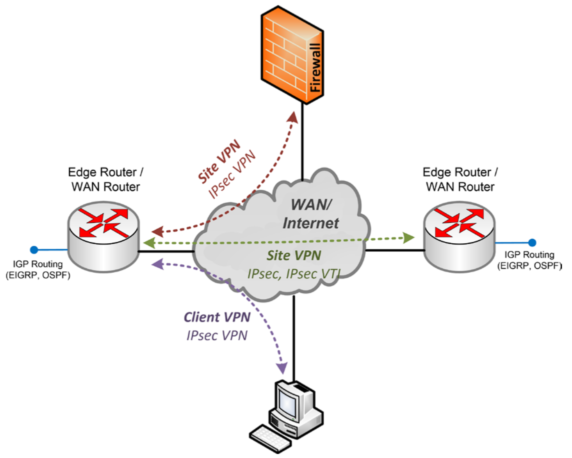
3.10.3.1 IPsec VPN

Select one (or more) of the following IPsec VPN PODs that will be used in the design:

🟩	**Deployment in WAN/Internet POD**		

Deployment in WAN/Internet POD

POD: SEC2-VPN-IPSEC-WANINET



- **When to use**: this is a standard deployment for IPsec between sites (or clients) over the Internet (or WAN) topology
- **Prerequisites**: SEC-NET-VPN-IPSEC
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: WAN router, Edge router, and/or Firewall appliance
- **Description**: in this POD, the WAN router (or VPN enabled network device) would build a point-to-point secure tunnel with another site using IPsec. This could be VPN tunnels established over the Internet or the WAN as shown in the picture above. Remote users, using VPN software, could also build a VPN tunnel back to the Edge router (or firewall appliance) to access network resources remotely.

Configuration

Below are the available options for deploying IPsec based on what is required:

	IPsec VPN If you require (1) building a few point-to-point VPN tunnels for accessing network resources securely between sites without using dynamic routing protocols. (2) To support a remote access solution using an installed VPN program to access network resources remotely.	**IPsec VTI / IPsec over GRE** If you require point-to-point VPN tunnels for accessing resources securely between sites. And supporting the use of dynamic routing protocols, multicast, and QoS	**L2TP over IPsec** If you require a remote access solution using a native VPN client to access network resources remotely. This doesn't require installing any additional VPN software on the client's system.

Below are required, recommended, and optional configuration when deploying IPsec on the network based on the available options:

Required	• **VPN Support**: based on the VPN enabled device (e.g. router, firewall) that will be used in the environment make sure it can support the IPsec VPN option that will be used. • **VPN Option**: determine the VPN option(s) that will be configured within the WAN/Internet POD

Recommended	• **Using Main Mode**: if you want to setup highly secure IPsec VPN tunnels by protecting the identity of the hosts, it is recommended to disable Aggressive mode. Aggressive mode does not protect the identity of the host setting up the VPN. It will send the host identities in clear-text across the network. Disabling Aggressive mode is what many security audits will recommend especially if the network is under a particular regulatory compliancy (e.g. SOX, PCI, HIPPA). • **NAT-T**: this option is configured when using IPsec for remote access. NAT-T provides support for IPsec traffic to travel through NAT enabled devices by encapsulating both the IPsec SA and the ISAKMP traffic in UDP packets. This option is enabled by default. • **MTU for IPsec VTI**: the safest and recommended MTU to use for GRE enabled interfaces to avoid fragmentation is 1400 bytes • **Pre-Fragmentation**: this feature is enabled globally (default) to increase the decrypting router's performance by using CEF switching (high performance) instead of process switching • **Path MTU Discovery (PMTU):** this is recommended to be implemented (if supported) to dynamically discover the smallest MTU size to use to avoid fragmentation • **Using IPsec VTI**: it is recommended to configure Tunnel mode (default) which supports pre-fragmentation which is ideal for large sized packets. Using Transport mode does not support pre-fragmentation, but saves 20 bytes compared to Tunnel mode.

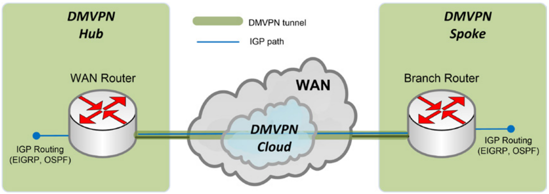
3.10.3.2 DMVPN

Select one (or more) of the following DMVPN PODs that will be used in the design:

🟩	**Single DMVPN Hub & Cloud**	**Dual DMVPN Hub + Single Cloud**	**Dual DMVPN Hub & Cloud**

Single DMVPN Hub and Cloud

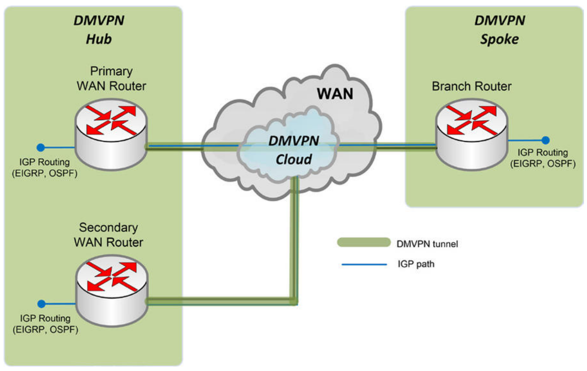
POD: SEC2-VPN-DMVPN-SHC



- **When to use**: if you are using a single WAN router at the main office (Hub) connected to a single Internet (or WAN) cloud
- **Prerequisites**: WAN-SRW, WAN-S-IWAN-VPN
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: DMVPN Hub, DMVPN Spoke(s)
- **Description**: in this POD, the main site is using a single WAN router acting as the DMVPN hub. It would be connected to a single Internet/WAN cloud. At the remote sites, the WAN routers (DMVPN spokes) would also connect to a single Internet/WAN cloud. They would be configured with a single mGRE tunnel interface pointing to the DMVPN hub. This POD is considered as a standard deployment for DMVPN as shown in the picture above.

Dual DMVPN Hub + Single Cloud

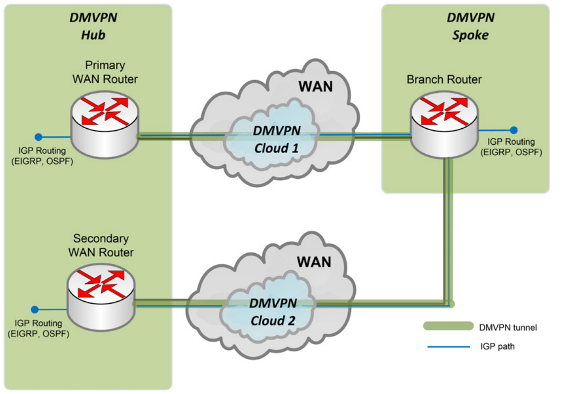
POD: SEC2-VPN-DMVPN-DH1C



- **When to use**: if you are using redundant WAN routers at the main office (Hub) connected to a single Internet (or WAN) cloud
- **Prerequisites**: WAN-DRSW, WAN-S-IWAN-VPN
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: DMVPN Hub, DMVPN Spoke(s)
- **Description**: in this POD, the main site is using two WAN routers (DMVPN hub) connected to a single WAN/Internet cloud. At the remote sites, the WAN routers (DMVPN spokes) would also connect to a single Internet/WAN cloud. In this topology, the two DMVPN hub routers would connect into the same logical DMVPN cloud using the same IP subnet as shown in the picture above. As a result, only one mGRE tunnel interface needs to be configured on the DMVPN spoke routers connecting to both of the DMVPN hub routers.

Dual DMVPN Hub and Cloud

POD: SEC2-VPN-DMVPN-DHC



- **When to use**: if you are using redundant WAN routers at the main office (Hub) connected to dual Internet (or WAN) clouds
- **Prerequisites**: WAN-DRW, WAN-D-IWAN
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: DMVPN Hub, DMVPN Spoke(s)
- **Description**: in this POD, the main site is using two WAN routers (DMVPN hub) connected to a different WAN/Internet cloud. At the remote sites, the WAN routers (DMVPN spokes) would also connect to an Internet/WAN cloud. In this topology, the two DMVPN hub routers would connect into one of the DMVPN clouds that will use its own IP subnet as shown in the picture above. This option is recommended for providing the best redundancy for DMVPN that rely on routing protocols inside of the VPN tunnels. However, the DMVPN spokes will need to use mGRE tunnel interfaces configured to each of the DMVPN Hub routers.

Configuration

Below are required, recommended, and optional configuration when deploying DMVPN services.

Required	• **DMVPN Hub**: determine and configure the DMVPN hub device(s) in the topology. This will be the WAN routers located at the main office or Data Center. • **DMVPN Spoke**: determine and configure all of the DMVPN spoke devices in the topology. This will be the WAN routers at the remote sites that will build a permanent connection to the DMVPN Hub and temporary connections (if needed) between the other sites.

Recommended	• **Routing Protocol**: it is recommended to use EIGRP instead of OSPF for the dynamic routing protocol • Use Dead Peer Detection (DPD) • Use Path MTU Discovery (PMTU) to reduce the amount of IPsec fragmentation • Use Digital Certificates (PKI) to provide better scalability if there are hundreds of DMVPN spokes • **Subnet Considerations**: it is recommended to use a /24 subnet for the DMVPN cloud if there will be ~254 remote sites. Or a /22 subnet if there will be ~400 remote sites. • **MTU**: the recommended MTU size to use for Tunnel interfaces to avoid fragmentation is 1400 bytes. Or you can use 1392 bytes (for unicast) or 1368 bytes (for multicast) if you are using MPLS over DMVPN. • **Call Admission Control (CAC) on DMVPN Spokes**: it is recommended to setup IKE CAC to avoid overloading the spoke routers. IKE CAC will limit the number of ISAKMP SAs to 25 (lower or higher as needed). Configure the System CAC to limit the number of SAs on the system to be 80% (lower or higher as needed).

Optional	• **GET VPN over DMVPN**: you can deploy DMVPN as the framework between all sites without encryption. GET VPN can be deployed on-top of the DMVPN topology to provide tunnel-less encryption between the sites. This will require adding GET VPN to the design.

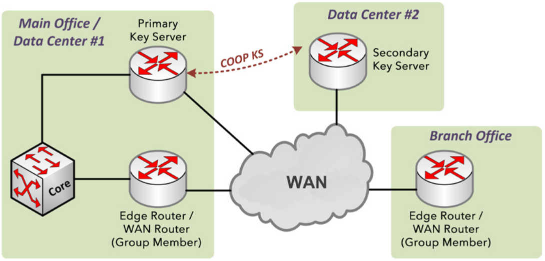
3.10.3.3 GET VPN

Select one (or more) of the following GET VPN PODs that will be used in the design:

🟩	**Deployment in WAN POD**		

Deployment in WAN POD

POD: SEC2-VPN-GETVPN-WAN



- **When to use**: this is a standard deployment for GET VPN enabled within the WAN POD
- **Prerequisites**: WAN-S-L3WAN, WAN-D-L3WAN, WAN-S-IWAN-LISP (using GET VPN over LISP), WAN-S-IWAN-VPN (using GET VPN over DMVPN), or WAN-D-L3WAN-IWAN-VPN (using GET VPN over DMVPN)
- **Required**: Cisco router
- **Has Sub-PODs**: --
- **Components**: Key Server(s), Group Members
- **Description**: in this POD, all of the WAN routers would be Group members. An additional router is required, a key server, which will be plugged into the L3 WAN. Redundant key servers (COOP KS) can also be deployed to provide high-availability to the WAN.

Configuration

Below are required, recommended, and optional configuration when deploying GET VPN services.

Required

- **Group Members**: determine all of the routers that will act as group members. They will be responsible for encrypting and decrypting traffic between the sites. The group members would be all of the WAN routers (hub and spoke) in the topology.
- **Key Server(s):** an additional router is added to the network and the WAN. The key server is responsible for authenticating the Group Members and managing the security policies for what traffic should be encrypted between the sites.

Recommended

- **Key Server Redundancy**: it is recommended to deploy redundant key servers which will operate in cooperative mode. They would become Cooperative key servers (COOP KSs) which will share the GDOI registrations for the group members.

Optional

- **GET VPN over LISP**: LISP is deployed as the framework between all sites without encryption. GET VPN can be deployed on-top of the LISP topology providing tunnel-less encryption between the sites. This will require adding LISP to the design.
- **GET VPN over OTP**: GET VPN can be configured with EIGRP OTP, which uses LISP, to provide encryption services.
- **GET VPN over DMVPN**: you can deploy DMVPN as the framework between all sites without encryption. GET VPN can be deployed on-top of the DMVPN topology to provide tunnel-less encryption between the sites. This will require adding DMVPN to the design.

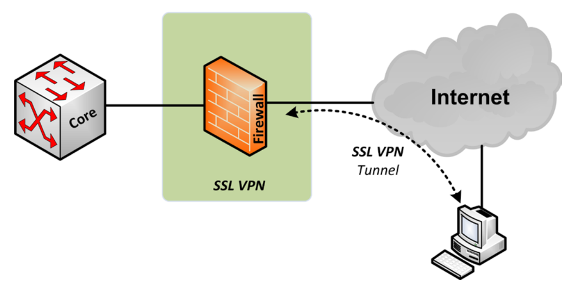
3.10.3.4 SSL VPN

Select one (or more) of the following SSL VPN PODs that will be used in the design:

🟩	**Deployment in Internet POD**		

Deployment in Internet POD

POD: SEC2-VPN-SSL-INET



- **When to use**: this is a standard deployment for SSL VPN to allow users to access network resources remotely over the Internet
- **Prerequisites**: INET, LAN/DC
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: Edge router (or Firewall appliance)
- **Description**: in this POD, users connected on the Internet would build a SSL tunnel to the Edge router (or firewall appliance) to access network resources remotely as shown in the picture above.

Configuration

Below are the available options for deploying SSL VPN based on what is required:

	Web Mode (Clientless) No VPN client app is installed. The user would simply use a web browser to access any web-based service through a secure web session.	**Tunnel Mode (SVC)** Client installs a SSL VPN program on their system which will establish a SSL VPN tunnel. This allows the client to access any network resource other than web-based applications.	

Below are required, recommended, and optional configuration when deploying SSL VPN services on the network based on the available options.

Required	• **Hardware**: it requires using router/firewall hardware that support SSL VPN (and its supported modes) • **SSL Mode**: determine what SSL VPN modes will be deployed on the edge router or firewall appliance

Recommended	• **SSL Mode using Web Mode**: if you require a VPN solution that doesn't involve installing VPN software on the user endpoints • **SSL Mode using Tunnel Mode**: if you require a VPN solution where the client can access any network resource (browser-based, native application) from any location on the Internet including Hotspot locations (e.g. Hotel, Airport, Coffee shops) using a basic Internet plan (if applicable).

Optional	• None Available

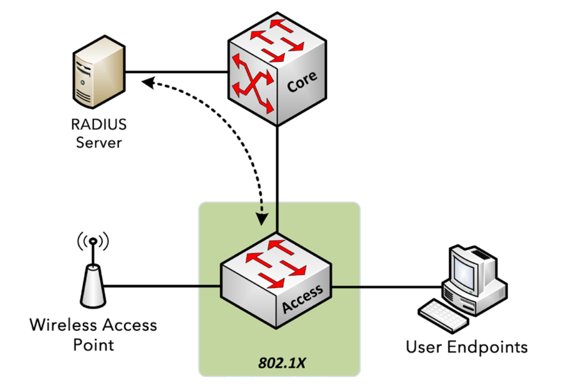
3.10.4 802.1x

Select one (or more) of the following 802.1X PODs that will be used in the design:

	Deployment in LAN POD		

Deployment in LAN POD

POD: SEC2-8021X-LAN



- **When to use**: if you require authenticating users on the LAN before they gain access to network resources
- **Prerequisites**: LAN
- **Required**: OPS-AUTH
- **Components**: LAN Access switches
- **Description**: in this POD, 802.1X would be enabled on the LAN Access switch and applied to one (or more) switch ports. The LAN access switch would also be configured for RADIUS which will point to a centralized authentication source for validating user authentication requests.

Configuration

Below are required, recommended, and optional configuration when deploying 802.1X services:

Required	• **Services**: using 802.1X requires implementing RADIUS services on the network device

Recommended	• **802.1X for Guest Users**: if a non-802.1x user is connected to an 802.1X enabled switch port or if they do not authenticate they will be placed into a Guest VLAN that is specified in the configuration • **Authentication Fail**: this is an option that is similar to the Guest option which specifies which VLAN a user who fails authentication will be placed into

Optional	• **MAC Authentication Bypass**: an option administrated from the RADIUS server that can bypass any user authentication via 802.1X using the MAC address of the connected system

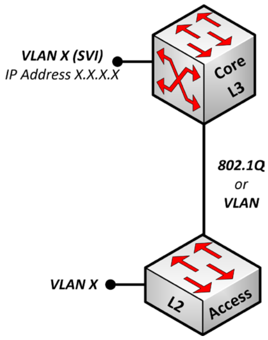
3.11 Switching

Select one of the following Switching PODs that will be used in the design:

	Hybrid Deployment	**Full Layer-2 Deployment**	**Full Layer-3 Deployment**

Hybrid Deployment

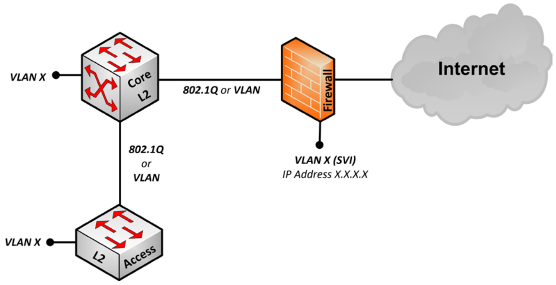
POD: SW-HYBRID



- **When to use**: if you require (1) using multiple VLANs across the entire network. And (2) if there will be inter-communication between the VLANs. This is important if you are using Wireless and Voice in the environment. This POD is commonly used compared to the other PODs listed.
- **Prerequisites**: LAN-2T (or LAN-3T), DC-2T
- **Required**: RT
- **Has Sub-PODs**: --
- **Description**: in this POD, a Layer-3 Core switch is used configured for routing and VLANs/802.1Q. Each VLAN (if required) will be configured with a Layer-3 VLAN interface (e.g. SVI) on the Core to allow inter-communication with other VLANs (e.g. Users, Server). The other switches in the topology such as the access switches would be a Layer-2 device configured with several VLANs. 802.1Q Trunking would be configured between all switches as shown in the picture above. Some of the switches could be added to a single VLAN if multiple VLANs do not need to be extended.

Full Layer-2 Deployment

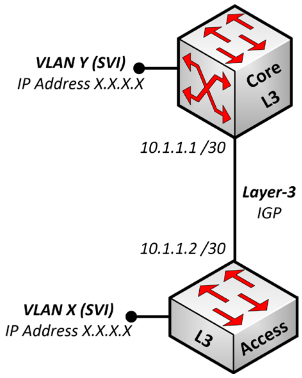
POD: SW-L2



- **When to use**: if you require (1) using one (or more) VLANs across the entire network. And (2) if there will be no (or little) inter-communication between the VLANs. This is more common for small-sized networks that don't want to use a Layer-3 Core switch due to cost.
- **Prerequisites**: LAN-2T (or LAN-3T), DC-2T, INET
- **Required**: RT
- **Has Sub-PODs**: --
- **Description**: in this POD, all of the network switches (e.g. Core switch, Access switches) are Layer-2 switches supporting only VLANs and 802.1Q Trunking. Each VLAN (if required) will be configured with a Layer-3 VLAN sub-interface (e.g. SVI) on the edge router/firewall appliance located in the Internet POD as shown in the picture above. 802.1Q Trunking would be configured between all switches if multiple VLANs need to be extended. Or those switches could be added to a single VLAN on the Core switch.

Full Layer-3 Deployment

POD: SW-L3



- **When to use**: if you require no VLANs to be extended across the network and/or to provide minimal Layer-2 configuration in the environment to avoid Layer-2 related outages (e.g. broadcast storm).
- **Prerequisites**: LAN-2T (or LAN-3T), DC-2T
- **Required**: RT (OSPF or EIGRP)
- **Has Sub-PODs**: --
- **Description**: in this POD, all of the network switches (e.g. Core switch, Access switches) would be Layer-3 switches supporting both routing and VLAN/802.1Q capabilities. Each VLAN (if required) will be configured with a Layer-3 VLAN interface (e.g. SVI) on its locally connected switch to allow inter-communication in the Layer-3 environment. Layer-3 interfaces would be configured between all of the switches as shown in the picture above. Any VLANs configured are confined to a single access switch or wiring closet. Furthermore, it is recommended to implement an IGP routing protocol (e.g. OSPF, EIGRP) among all of the Layer-3 network devices in the environment.

Configuration

Below are required, recommended, and optional configuration when deploying Switching services.

Required

- **Trunking using 802.1Q**: if more than one VLAN will be used across the network then 802.1Q Trunking should be configured on interfaces between the switches. Including other devices that require supporting multiple VLANs.
- **VLAN Trunking Protocol (VTP):** specify a VTP domain name and use VTP Transparent mode on all switches in the topology to avoid configuration revision meltdowns.
- **Virtual LAN (VLAN):** add all of the VLANs based on the networks that will be used
- **Spanning Tree Protocol (STP):** it is required to enable STP on all switches in the environment to prevent loops and broadcast storms. It is recommended to enable Rapid Spanning Tree (802.11w) instead of legacy STP as it provides fast convergence (~900ms) in the event of a failure on the Layer-2 network.
- **Extended VLANs**: if 1000 to 4000 VLANs will be used on the network then the system ID needs to be extended on all Layer-2/Layer-3 switches, which is something that is configured with the Spanning Tree Protocol (STP).

Recommended (1/2)

- Do not use VLAN1 (the default)
- Use separate VLANs for Data and Voice traffic
- As a best practice configure a small set of VLANs per switch (<30 VLANs should be created)
- Create user VLANs per Department, Building, Floor, or Quadrant
- **VTP Transparent Mode**: it is recommended to implement VTP transparent mode on all switches in the topology as outlined in the requirements section. The drawback is that VLANs are administered for each device, but it avoids losing an entire VLAN (hence subnet) on the network that can occur when using VTP Server and Client modes. In transparent mode, adding (or removing) VLANs is done manually on each Layer-2 device where needed.
- **VLAN Trunk Security**: it's a good practice to allow only the VLANs that are needed for a device (e.g. Wireless AP, switch) and nothing more. For example, if the WLAN uses only two VLANs then only those VLANs should be allowed to the access points.
- **Dynamic Trunk Port (DTP):** as a best practice configure DTP to not negotiate and trust the encapsulation protocol that is used for the Trunking interface, which is 802.1Q. This will put the port into a permanent Trunking mode and will not allow the port to generate DTP frames. In general, always try to avoid any type of protocol negotiation between critical devices.
- **Native VLAN for Trunking Ports**: the Native VLAN is the only VLAN that is untagged and can be exploited in VLAN Hopping attacks. Therefore, as a best practice configure the native VLAN for 802.1Q ports to use a bit-bucket VLAN (e.g. VLAN999) that is in a shutdown state and not routable with other networks/VLANs.
- **Root Bridge**: each VLAN configured on the network must use a Layer-2/Layer-3 switch to be the root bridge. It is recommended to implement the root bridge on the Core (in a tier-2 topology) or the Distribution (in a tier-3 topology).
- **Root Guard**: it is recommended to configure Root Guard on all downlink ports to the LAN access switches to prevent the port in becoming a root port, hence, acting as the root bridge on the Layer-2 network.
- **Loop Guard**: enabled globally on all Access and Core switches to prevent a blocked port from transitioning to listening after the MaxAge timer has expired. This should be implemented if Bridge Assurance is not supported on the switch.
- **Source Guard**: to protect against IP address spoofing attacks on the network. This feature should be configured on all Access Switches.

Recommended (2/2)

- **Broadcast Suppression**: to avoid the spread of a broadcast storm it is important to control the amount of broadcast traffic across the Layer-2 network. Broadcast suppression should be configured on downlink ports towards the LAN Access switches since a broadcast storm is more likely to be caused by a user endpoint creating a loop. For the percentage, most environments can start with 20% and adjust (up or down) as needed.
- **BPDU Guard / Filter**: BPDU Guard can be used on endpoint switch ports to prevent unauthorized (rogue) switches being plugged into the network. This is recommended to prevent possible global switching failures and should be enabled globally on all Access Switches. An alternative would be to filter inbound and outbound BPDU messages. This feature is good for implementing on known edge ports or switches you don't want to include as part of your Layer-2 domain.
- **Bridge Assurance (BA)**: deals with what ports should send BPDU messages when STP PortFast is configured. It is recommended to enable the endpoint ports for "***PortFast Edge***" and the uplink/downlink ports for "***PortFast Network***". However, as a best practice it is recommended to set the global default to "***Network***" which helps to avoid unidirectional links and potential software issues. These recommendations also apply for Cisco Nexus series hardware.
- **DHCP Snooping**: used to prevent rogue DHCP servers from being plugged into the network that is not trusted which can cause DHCP starvation attacks. DHCP snooping should be enabled on the LAN Access switches where DHCP services should not exist. Make sure to mark all uplink/downlink switch ports on the Access switches to be "trusted". Lastly, DHCP snooping inspection should be rate limited to "100" to protect the control plane and the switch itself.
- **Dynamic ARP Inspection (DAI):** prevents against ARP spoofing, poisoning, and starvation on the network. This feature should be configured on all Access Switches. It should be rate limited to "100" to protect the control plane and the switch itself. And make sure to mark all uplink/downlink switch ports on the Access switch to be "trusted".
- **ARP Aging/Timeout**: tune ARP aging timers close or equal to the CAM/MAC-address aging value (default is 200 seconds). The default ARP age/timeout is 4 hours, so tune the timeout to be 200 seconds.

Optional

- **Port Security:** used to allow a specific host to be connected to a dedicated switch port based on the MAC address (also called a secure MAC address). Or to limit the number of MAC addresses that can be active on a switch port. The secure MAC address can be configured statically on the switch port or it can dynamically learn the addresses (called "sticky addresses"). This will help against CAM attacks (e.g. MAC flooding) and DHCP starvation.
- **Flex Link**: a locally significant feature that creates a primary and backup switch port on a Layer-2/Layer-3 switch. This is an optional feature that can be implemented on Access switches if it is supported. For the configuration, specify the primary uplink to the Core/Distribution switch to be the primary port. The secondary Core/Distribution switch that the Access switch is connected to would be the backup port. Keep in mind that this feature does not create a loop-free network, so using STP is still recommended for the design.
- **Uplink Fast**: enable on Access switches to quickly move a blocked port to a forwarding port automatically if there is a link failure when the switch doesn't support Rapid Spanning Tree.
- **STP Path Cost**: change the STP Path Cost method to "long" globally on Data Center switches (LAN Switches can also be considered). This causes STP to use 32-bit based values when determining the port path cost compared to the default 16-bit value which improves the root path selection when a Port Channel using PAgP is configured.
- **Protected Ports**: an optional feature configured on switch ports to prohibit communication with other protected switch ports on the local switch in the same VLAN. Communication with non-protected ports within the same VLAN is allowed. This feature does not provide isolation of protected ports located on different switches.
- **Private VLANs**: optional feature that can create sub-VLANs within a single VLAN. Private VLANs are used to provide stronger security between hosts in the same VLAN. This is an uncommon VLAN mechanism deployed in LAN/Data Center switching environments unless unique security requirements are required.

3.12 Virtualization

Select one (or more) of the following virtualization PODs that will be used in the design:

	Virtual Routing & Forwarding (VRF)	**Network Functions Virtualization (NFV)**	**L3VPN - MPLS**
	L2VPN – Metro Ethernet		

Virtual Routing & Forwarding (VRF)

POD: VRT-VRF

- **When to use**: if you require creating virtual isolated routers across the network
- **Prerequisites**: VRT, LAN/DC
- **Required**: --
- **Has Sub-PODs**: Go to 3.12.1

Network Functions Virtualization (NFV)

POD: VRT-NFV

- **When to use**: if you require virtualizing various network functions (e.g. routing, firewall, load-balancing) to be used for different customer networks
- **Prerequisites**: VRT
- **Required**: --
- **Has Sub-PODs**: --

L3VPN - MPLS

POD: VRT-L3VPN

- **When to use**: used on a service provider network to connect customer networks together and be isolated from other customer domains. This will provide traffic and route separation between the customer networks.
- **Prerequisites**: VRT, SP
- **Required**: --
- **Has Sub-PODs**: Go to 3.12.2

L2VPN – Metro Ethernet

POD: VRT-L2VPN

- **When to use**: used on a service provider network to extend VLANs between customer sites and be isolated from other customer domains
- **Prerequisites**: VRT, SP
- **Required**: --
- **Has Sub-PODs**: Go to 3.12.3

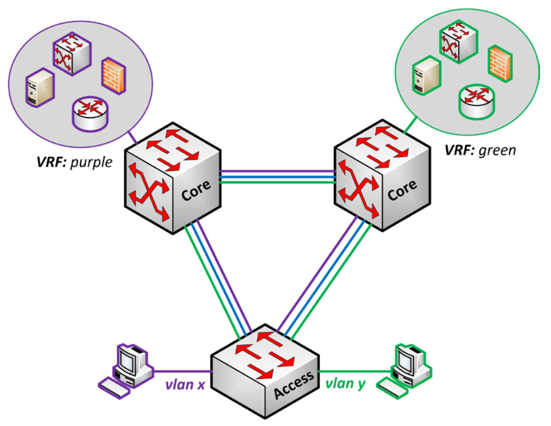
3.12.1 Virtual Routing & Forwarding

Select one of the following VRF PODs that will be used in the design:

	Standard Deployment	**Deployment with Zone Router**	

Standard Deployment

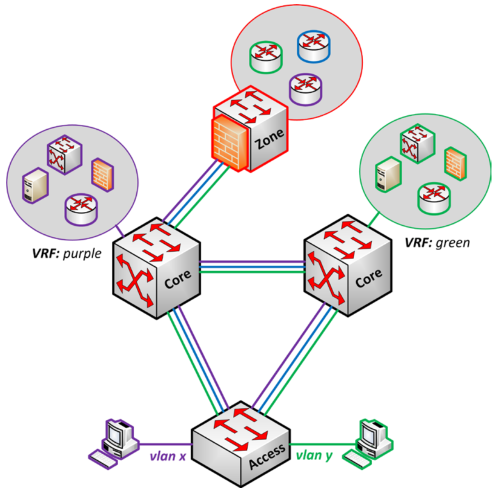
POD: VRT-VRF-STD



- **When to use**: if you require creating isolated virtual networks with no routing between other virtual networks
- **Prerequisites**: --
- **Required**: VRF-enabled hardware
- **Has Sub-PODs**: --
- **Description**: in this POD, a VRF instance is created on all supported network devices for each virtual network. VLANs and 802.1Q Trunking are used for extending that isolated network between the other VRF-enabled network devices as shown in the picture above. It's important to note that implementing VRF does not encrypt traffic across the network.

Deployment with Zone Router

POD: VRT-VRF-ZR



- **When to use**: if you require creating isolated virtual networks with the ability to allow routing between other virtual networks
- **Prerequisites**: --
- **Required**: VRF-enabled hardware
- **Has Sub-PODs**: --
- **Description**: in this POD, a VRF instance is created on all supported network devices for each virtual network. VLANs and 802.1Q Trunking are used for extending that isolated network between the other VRF-enabled network devices. An additional Layer-3 device, a Zone router is added to the topology to act as a transit for access between the isolated networks as shown in the picture above. A firewall appliance is placed in-line with the Zone router to provide security enforcement between the virtual networks. It's important to note that implementing VRF does not encrypt traffic across the network.

Configuration

Below are the available options for deploying VRF based on what is required

	Easy Virtual Network (EVN) An enhancement to VRF-lite where a VNET trunk can be defined on interfaces to extend a VRF instance across the network with minimal configuration required. It supports up to 32 virtual networks per platform.	**Multi-CE VRF (VRF-lite)** VRF technology that requires creating VRF instances on each network device. Then using VLANs, SVI, and 802.1Q configuration to extend a VRF instance across the network.

Below are required, recommended, and optional configuration when deploying VRF services on the network based on the available options:

Required	• **Hardware**: it requires using Cisco hardware that support EVN or VRF-lite services such as the Cisco ISR and ASR series • **VRF Definition**: define all of the VRF instances (virtual networks) that will be used on the network. Each VRF should be configured on each VRF-enabled device globally in the topology. • **Assign VRF to Interfaces**: assign the VRF to all of the necessary Layer-3 interfaces that will be part of a particular virtual network • **VNET Trunk**: enable VNET Trunking on all uplink/downlink ports in the topology to support extending the virtual network (VRF) across the LAN/DC. This will automatically create sub-interfaces for each VRF instance that is added to a EVN enabled device. The sub-interfaces cannot be created manually. Each sub-interface inherits the same characteristics from the main interface that is configured. • **Routing Protocol**: each VRF instance should be configured with a routing protocol supporting VRF such as OSPF or EIGRP.

Recommended	• **Using Easy Virtual Network (EVN):** it is recommended to use EVN instead of VRF-lite to minimize the overall configuration required. EVN can also virtualize the control-plane and data-plane for each VRF instance per platform allowing a hop-by-hop data path through the network. • EVN is backwards compatible with VRF-Lite. However, the 802.1Q tag (used with VRF-lite) and the VNET tag (used on the EVN-enabled device) must match between the connected network devices. • When creating a VRF name do not use the name "global" • **VNET List**: it is recommended to implement VNET trunk security to specify what VRFs are allowed across an interface. This feature works similar to 802.1Q trunk security. VNET trunk security must be configured equally between the connected devices. • **VRF and Voice using Cisco CME**: VRF and Cisco CME cannot be configured together on the same router platform. It is recommended to use a single WAN branch router where VRFs exist for all networks except for voice, which is not in a VRF.

Optional	• **Route Replication**: if you require sharing routes between VRFs and will use Cisco EVN. You can use a feature called "Route Replication" to specify what routes within a VRF can be redistributed into another VRF instance. This does not require route targets, imports, nor exports under the VRF definition. • **Routing and Security between VRFs**: if you require routing between the isolated VRF instances you can add a Zone router to the topology. This router is not enabled for VRF and will contains all routes on the network. A firewall appliance would then be placed in-line between the Zone router and the Core switch (LAN or Data Center) to provide security enforcement between the virtual networks. The interface on the Zone router connected into the Core would be a 802.1Q trunk interface with multiple VLAN tags. Each of those VLAN will have an SVI which would be associated to a VRF instance on the Core switch. This is important for send routing information within a VRF up to the Zone router. • **DMVPN per VRF**: used to extend a VRF across a DMVPN network using VRF-lite. The WAN routers would be treated as CE/PE devices.

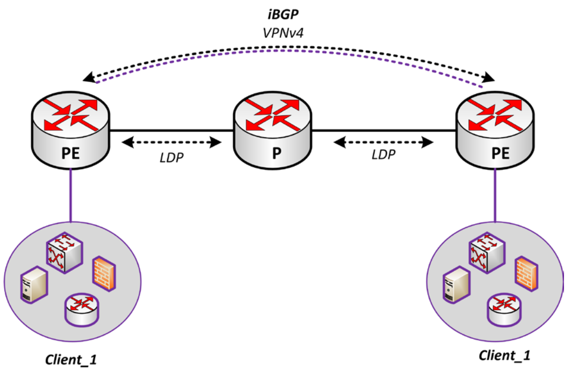
3.12.2 L3VPN - MPLS

Select one of the following MPLS PODs that will be used in the design:

	Traditional MPLS	Unified MPLS	

Traditional MPLS

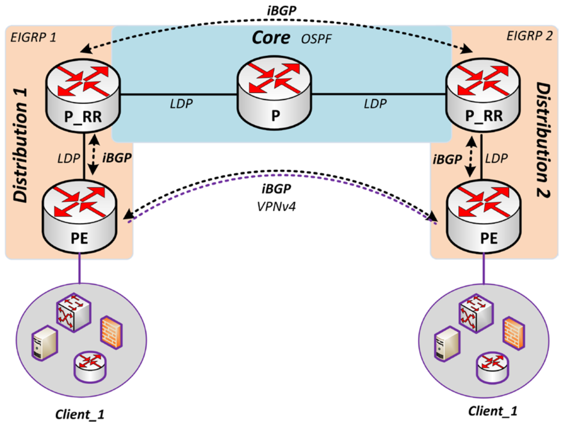
POD: VRT-L3VPN-MPLS



- **When to use**: if you require a standard deployment of MPLS in a service provider network (medium or large)
- **Prerequisites**: SP
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: MPLS routers (P, PE)
- **Description**: in this POD, the service provider network consist of several MPLS routers enabled for LDP, IGP, and MP-BGP. This is the simplest deployment of MPLS as shown in the picture above. It's important to note that implementing MPLS does not encrypt traffic across the network.

Unified MPLS

POD: VRT-L3VPN-UMPLS



- **When to use**: if you require a scalable deployment of MPLS to support a high number of clients in a service provider network (large). It will also provide faster convergence in the topology.
- **Prerequisites**: SP
- **Required**: --
- **Has Sub-PODs**: --
- **Components**: MPLS routers (P, PE), Route Reflectors (RR)
- **Description**: this POD will resemble a Traditional MPLS but with hierarchical parts of a core and distribution layer as shown in the picture above. PE routers would exist in different distribution blocks with a local MPLS Provider RR. Each RR would also be connected into the Core layer. Furthermore, each distribution block will run its own IGP separate from the other distributions and the core itself. The entire Unified MPLS topology will exist in a single BGP ASN. This will be used for building MP-BGP connections between some of the other PE routers. It's important to note that implementing MPLS does not encrypt traffic across the network.

Configuration

Below are required, recommended, and optional configuration when deploying MPLS services:

Required	• **MPLS Provider Edge (PE):** determine all of the MPLS routers that will be directly connected to a customer site (CE) and into the MPLS network. These would be considered as Provider Edge (PE) routers. The VRF instances would be configured directly on the PE routers and will use MP-BGP for communicating with other PE routers to exchange VRF routing information. The MPLS PE is considered as the access layer in the MPLS topology with client facing networks. • **MPLS Provider (P):** any MPLS router in the topology that isn't directly connected to a customer site, but used as a transit across the MPLS is considered as a Provider (P) router. They will connect to PE and other P routers making up the MPLS Backbone. VRF's are not configured on the P routers, only LDP is configured for extending the MPLS labels between the routers. • **IGP Routing Protocol**: an IGP routing protocol (EIGRP, OSPF, IS-IS) is required to be configured on the network between the MPLS routers. This is important for the MPLS PE routers to establish MP-BGP connections. It is recommended to use either OSPF or IS-IS especially if Traffic Engineering will be implemented across the MPLS network. • **Label Switching**: a label distribution protocol (e.g. LDP) is required on all MPLS router interfaces. This will be used for forwarding labels between the MPLS routers. • **MP-BGP between PE**: IBGP peering is required between MPLS PE routers to exchange VPNv4 routes for a VRF instance that is associated to a customer site. • **VRF**: each customer network will be configured as a VRF creating an isolated routing table on the network device and supporting overlapping address ranges. The VRF is only configured on the MPLS PE routers and will be associated to the downlink port connected to a customer site. • **Route Reflector in Unified MPLS**: a BGP reflector router is deployed in each distribution block in a Unified MPLS topology. They would peer with local PE routers in its distribution block, but it will also connect the distribution block into the core of the MPLS network. The RR routers are used for allocating labels and communicating with the other distribution blocks. It is also responsible for changing the next-hop address used by the PE routers to reach the other parts of the MPLS network.

Recommended	• **VRF RD Naming Standard**: it is recommended to create a naming standard for naming the VRF Route Distinguishers (RD) on the network • **Loopback Interfaces**: it is recommended to configure loopback interfaces on all of the MPLS routers. This should be used for all LDP, IGP, and MP-BGP peering among the MPLS routers • **Route Reflectors in Traditional MPLS**: it is recommended for all PE routers to peer with a dedicated BGP router that is configured as a route reflector. This will provide better scalability, management, and redundancy for IBGP peering between the PE routers. The route reflectors would be connected into the Core of the MPLS network. • **MTU Considerations:** using MPLS VPN tunneling will introduce additional overhead across the network. It is recommended to use Jumbo Frames if supported over the MPLS topology.

Optional	• **VRF Selection**: a feature used to support multiple VRFs on a single interface • **Traffic Engineering**: to provide IntServ QoS to create tunnels along an LSP through the MPLS network using OSPF/IS-IS extensions. The tunnels can be configured statically along a specified path of MPLS routers. Or dynamically based on the bandwidth resources available using RSVP. It also provides fast reroute mechanisms to detect failures and create backup LSPs if resources are available. • **MPLS MTU**: this feature should be set for GRE-enabled interfaces configured on the MPLS network • **MTU with MPLS over DMVPN**: the recommended MTU to use for GRE interfaces to avoid fragmentation would be 1392 bytes (for unicast) or 1368 bytes (for multicast). This is applicable when using MPLS over DMVPN. • **Quality of Service (QoS)**: this is required if customer networks will mark packets locally within their network and will be sent across the MPLS. The MPLS network can be implemented for Uniform, Short Pipe, or Pipe mode depending on what QoS operation is required. • **Route Target Constraint (RTC):** an optional feature used to restrict what routes are received from other PE routers. This is recommended for scalable MPLS environments with Route Reflectors. The RR will implement outbound filtering to send the necessary routes to another PE router based on its route target configuration.

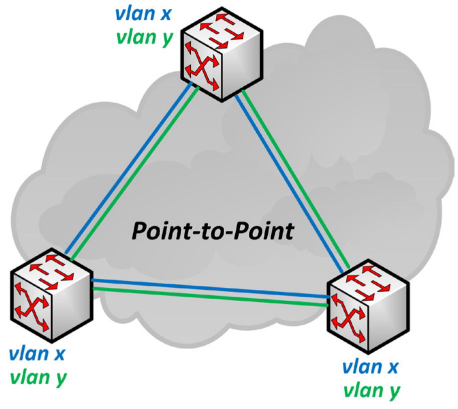
3.12.3 L2VPN – Metro Ethernet

Select one (or more) of the following L2VPN PODs that will be used in the design:

	L2VPN over MPLS	**VPLS over MPLS**	**802.1Q Tunneling (Q-in-Q)**

L2VPN over MPLS

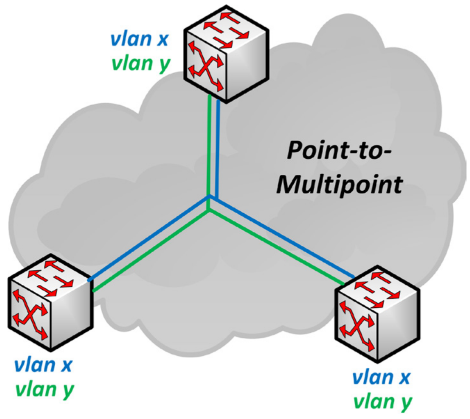
POD: VRT-L2VPN-L2VPN



- **When to use**: if you require building Layer-2 point-to-point connections between two customer sites across the existing MPLS network
- **Prerequisites**: VRT-L3VPN
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: in this POD, the L2VPN topology would overlay on-top of the existing MPLS network already built. There are several different Layer-2 point-to-point technologies that can be used. They include Ethernet over MPLS (EoMPLS, AToM), L2TPv3, VPWS, EPL (Port-Based), and EVPL (VLAN-based).

VPLS over MPLS

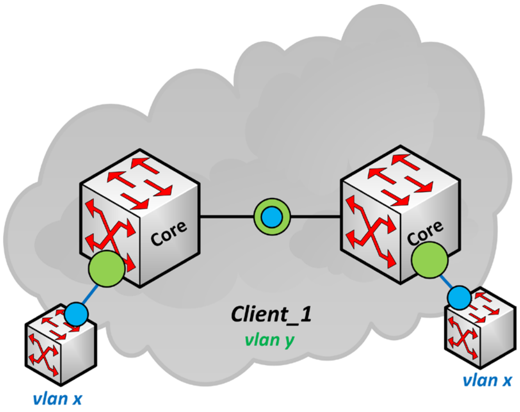
POD: VRT-L2VPN-VPLS



- **When to use**: if you require building a mesh (point-to-multipoint) of Layer-2 connections between multiple customer sites across the existing MPLS network
- **Prerequisites**: VRT-L3VPN
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: in this POD, the L2VPN topology would overlay on-top of the existing MPLS network already built. There are several different Layer-2 point-to-multipoint technologies that can be used. They include VPLS, EPLAN (Port-Based), and EVPLAN (VLAN-based). There are considerations to keep in mind which include the MAC address table size and flooding of unknown frames across the service provider network. These could affect the overall performance and reliability of the L2VPN infrastructure.

802.1Q Tunneling (Q-in-Q)

POD: VRT-L2VPN-QINQ



- **When to use**: if you require building Layer-2 point-to-point connections between two customer sites over an existing switching topology supporting VLANs and 802.1Q Trunking
- **Prerequisites**: SW
- **Required**: --
- **Has Sub-PODs**: --
- **Description**: in this POD, 802.1Q Trunking is enabled throughout the service provider network. All traffic/frames for a customer would be encapsulated inside of a unique VLAN tag which would be extended across the network to another customer site.

4. Attributes

Select one (or more) of the following attributes that will be used in the design:

Locations	**Connections**	**Networks**
Standards	**Resources**	

Locations

POD: ATT-LOC

- **When to use**: to determine the location for each network device used in the topology
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 4.1

Connections

POD: ATT-CON

- **When to use**: to determine what network connections and bandwidth services is required for the various components on the network
- **Prerequisites**: ATT-LOC, LAN/DC, INET, WAN
- **Required**: --
- **Has Sub-PODs**: Go to 4.2

Networks

POD: ATT-NET

- **When to use**: to determine the type of networks that will be used in the topology
- **Prerequisites**: LAN/DC, INET
- **Required**: --
- **Has Sub-PODs**: Go to 4.3

Standards

POD: ATT-STD

- **When to use**: to determine what standards will be used on the network for better organization
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 4.4

Resources

POD: ATT-RES

- **When to use**: additional design resources that can be referenced
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 4.5

4.1 Locations

Complete each of the following PODs to determine all of the rooms, buildings, and locations that will be used on the network:

	Local Area Locations	**Wide Area Locations**	

Local Area Locations
POD: ATT-LOC-LOCAL
• **When to use**: this is required to determine where the network devices will be located in the building(s) • **Prerequisites**: -- • **Required**: -- • **Has Sub-PODs**: Go to 4.1.1

Wide Area Locations
POD: ATT-LOC-WIDE
• **When to use**: if the network will have multiple sites/locations • **Prerequisites**: -- • **Required**: WAN • **Has Sub-PODs**: Go to 4.1.2

4.1.1 Local Area Locations

For each building determine what type of rooms exist and how they will be connected together based on the topology that will be used:

Local Area Locations	**Data Center** A dedicated room that consist of servers, racks, cabinets, server patch panels, and other data center facility components. A Data Center may be wired directly to an MDF and/or IDF closets. Internet and WAN circuits could also be terminated in the Data Center if they are extended from the MPOE.	**Wiring Closet (IDF)** A wiring closet that is wired (fiber or copper) back to the MDF room. IDF wiring usually occurs from the user workspace, cubicle, and/or office to patch-panels in the IDF room. Some IDF rooms may be wired between each other or directly to the Data Center.
	MDF, BDF A wiring closet connecting to multiple IDF rooms and Data Center (if applicable). A MDF may have Internet and WAN circuits terminated if they are extended from the MPOE.	**MPOE** This will be a room/location where external circuits are terminated before being extended to a Data Center and/or MDF room.
	Lab Similar to a Data Center, but dedicated for testing or lab devices that may be wired back to a Data Center, MDF, and/or IDF.	**Classroom** A classroom location that consist of students with multiple computer systems. Either individual ports could be wired back to a MDF, IDF, or Data Center through a patch panel. Or using a single cable (or more) leading back to a MDF, IDF, or Data Center where the classroom has a dedicated switch that all computer devices would be connect to.
	Custom Any other computer or wiring room consisting of network equipment not easily placed in any of the other local room locations.	

4.1.2 Wide Area Locations

Determine what type of locations will be connected to the WAN based on the topology that will be used:

Wide Area Locations	**Hub (Main Office)** Determine the main office that will connect into the WAN. This could be the HQ site or location where network resources will be accessed by the branch offices.	**Remote Office / Branch Office (ROBO)** Determine the number of remote sites that will connect into the WAN. This would be smaller offices that would access network resources located at the main office and/or Data Center.
	Data Center Determine if a dedicated Data Center location will be connected into the WAN. The Data Center will consist of servers accessed by users at the main and branch offices. This can also be considered as a Disaster Recovery site for the environment.	**Custom** Any site that isn't classified as a main office, branch office, or Data Center that will be connected into the WAN.

4.2 Connections

Complete each of the following PODs to build the connections and bandwidth services between the network devices in the design:

	Connection Deployment	**Bandwidth Services**	

Connection Deployment

POD: ATT-CON-DEPLOY

- **When to use**: for each network device in the topology, determine all of the different port types that will exist on that device
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 4.2.1

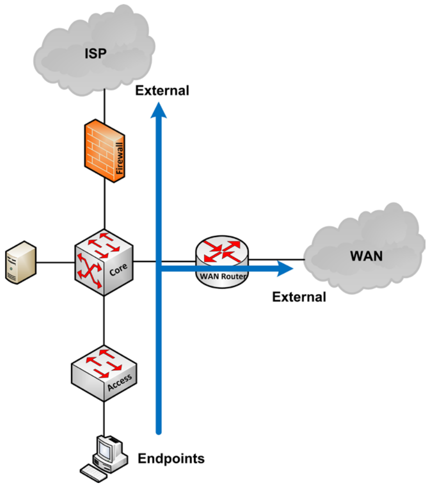
Bandwidth Services

POD: ATT-CON-BW

- **When to use**: based on the connection deployment determine the bandwidth service for all ports on each network device
- **Prerequisites**: ATT-CON-DEPLOY
- **Required**: --
- **Has Sub-PODs**: Go to 4.2.2

4.2.1 Connection Deployment

In the topology, the flow of the network goes from the endpoint up to the Internet and/or WAN in the environment. Therefore, the ports for some of the network devices will have uplinks which are ports that are connected up towards the Internet/WAN. And some ports on the network devices may have downlinks which are ports that are connected down towards the endpoints. This flow is reflected in the picture on the right:

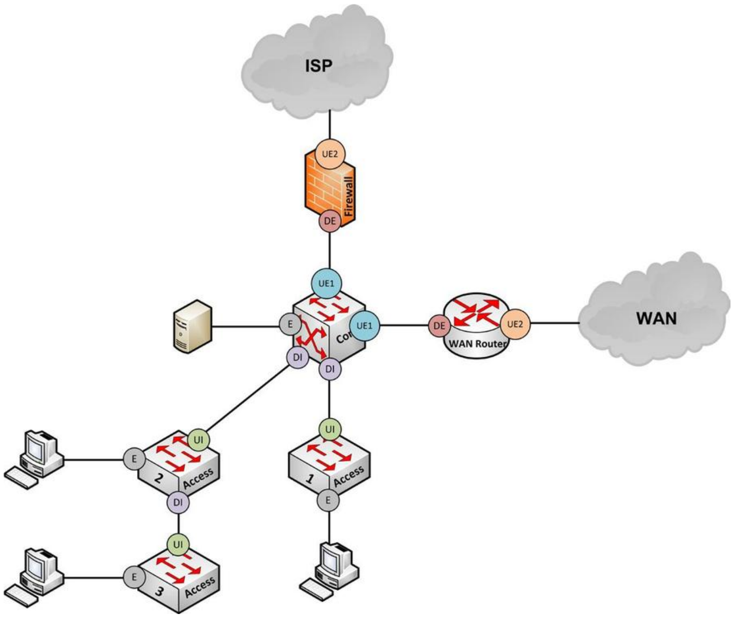


For each network device in the topology, determine all of the different port types that will exist. Below are the possible port types that can be identified:

Internal Port Types	External Port Types
Internal Uplink Ports (UI ports) These are ports that connect up to another switch within the LAN/DC	**External Uplink 1 Ports (UE1 ports)** These are ports that connect up to a network device that has UE2 port(s)
Internal Downlink Ports (DI ports) These are ports that connect down to another switch within the LAN/DC	**External Uplink 2 Ports (UE2 ports)** These are ports on a network device located in the Internet or WAN POD that connect up to a service provider (e.g. ISP cloud, WAN cloud)
Edge Ports (E ports) These are ports on a network device that has an endpoint connected	**External Downlink Ports (DE ports)** These are ports on a network device located in the Internet or WAN POD that connects down towards the LAN/DC

Example

Look at the following diagram below. It is a simple topology that shows how to identity the ports on each network device:



- **Firewall Device**: this device will have UE2 and DE ports. The UE2 port would connect up to the ISP cloud. And the DE port would connect down towards the LAN/DC, in this case, the Core switch.
- **Core Switch**: this device will have a mix of DI, UE1, and E ports. The UE1 port would connect up to the firewall since that device is located in the Internet POD. And another UE1 port connected to the WAN router. The DI ports would connect down to each of the access switches. And there will be servers directly connected to this device. So those ports would be identified as E ports.
- **Access Switch #1**: this device will have UI and E ports. Its UI port will connect up to the Core switch. And the E ports is where the user endpoints would be connected.
- **Access Switch #2**: this device will have UI, DI, and E ports. The UI port would connect up to the Core switch. But it will also have downlink ports to another switch, so that port would be identified as a DI port. This device would also have E ports that will have user endpoints connected.
- **Access Switch #3**: this device will mirror Access Switch #1. It will have UI and E ports. Its UI port will connect up to Access Switch #2. And the E ports is where the user endpoints would be connected.
- **WAN Router**: this device would be similar to the firewall appliance, but this device is located in the WAN POD. This device will have UE2 and DE ports. Its UE port would connect up to the WAN cloud. And its DE port would connect down to the Core switch.

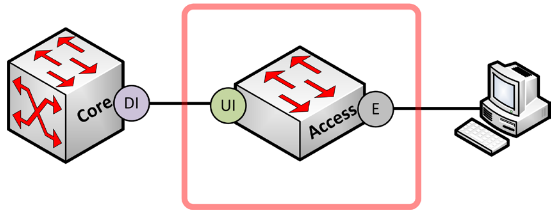
This example topology will be referenced throughout this section.

For each network device select one of the following PODs based on the type of ports it will have:

	UI Port Deployment	**UI and DI Port Deployment**	**UE1 and DI Port Deployment**
	UE2 and DE Port Deployment	**UE1 and DE Port Deployment**	**UE Port Deployment**

UI Port Deployment

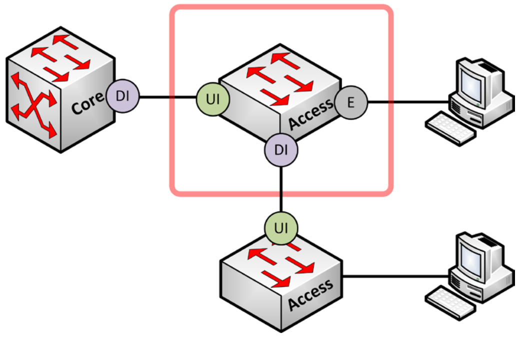
POD: ATT-CON-DEPLOY-UI



- **When to use**: if the network device only has internal Uplink ports. This will either be an access switch or some custom/standard switch.
- **Prerequisites**: --
- **Required**: ATT-CON-BW-UI, ATT-CON-BW-E
- **Description**: in this deployment, the access switch (or standard/custom switch) will have uplinks port(s) connected up to the Core switch as shown in the picture above. The access switch will also have edge ports with connected endpoints (e.g. user, server).

UI and DI Port Deployment

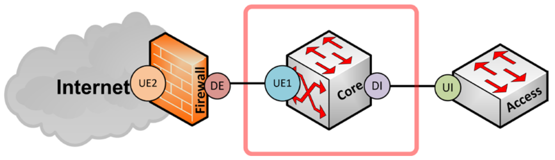
POD: ATT-CON-DEPLOY-UI-DI



- **When to use**: if the network device has internal Uplink and Downlink ports. This will either be (1) a Distribution switch in a 3-tier topology. Or (2) an access switch within a group of daisy-chained switches (not recommended).
- **Prerequisites**: --
- **Required**: ATT-CON-BW-UI, ATT-CON-BW-DI, ATT-CON-BW-E (if applicable)
- **Description**: in this deployment, the distribution switch (or access switch within a daisy-chain) will have an uplink port(s) connected up to the Core switch as shown in the picture above. The switch would also have a downlink ports(s) connected down to access switches (or other switches).

UE1 and DI Port Deployment

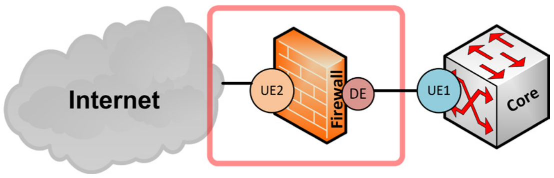
POD: ATT-CON-DEPLOY-UE1-DI



- **When to use**: if the network device has an internal Downlink port and an external Uplink port. This will likely be the Core switch in the topology.
- **Prerequisites**: --
- **Required**: ATT-CON-BW-UE1-DE, ATT-CON-BW-DI, ATT-CON-BW-E (if applicable)
- **Description**: in this deployment, the Core switch (in a 2-tier or 3-tier topology) will have downlink port(s) to access switches. The Core switch will also have an external Uplink connected to an external device which could be a WAN router, Edge router, and/or Firewall appliance as shown in the picture above.

UE2 and DE Port Deployment

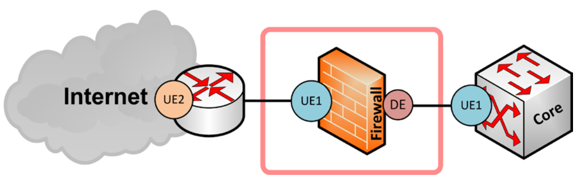
POD: ATT-CON-DEPLOY-UE2-DE



- **When to use**: if the network device has external Uplink and Downlink ports. This will either be a WAN router, Edge router, or Firewall appliance that is directly connected into the Internet/WAN cloud.
- **Prerequisites**: --
- **Required**: ATT-CON-BW-UE2, ATT-CON-BW-UE1-DE
- **Description**: in this deployment, the network device will have an external uplink port(s) connected to a service provider (e.g. Internet, WAN) as shown in the picture above. It will also have an external downlink port connected to the Core switch. Or to another network device within the Internet/WAN POD such as a firewall appliance.

UE1 and DE Port Deployment

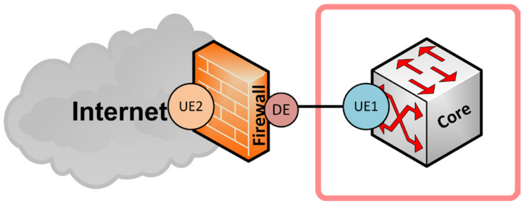
POD: ATT-CON-DEPLOY-UE1-DE



- **When to use**: if the network device exists within the Internet/WAN POD and is directly connected to a network device that has a UE2 port. This will be a network device that is in-line between the WAN/Internet devices and the LAN/DC (e.g. firewall, WAN optimization appliance)
- **Prerequisites**: --
- **Required**: ATT-CON-BW-UE1-DE
- **Description**: in this deployment, a network device would be in-line between the Internet/WAN and the LAN/DC network as shown in the picture above. This device could be a firewall appliance that is in-line between the edge router and the LAN/DC. Or a WAN optimization appliance in-line between the WAN router and the LAN/DC.

UE1 Port Deployment

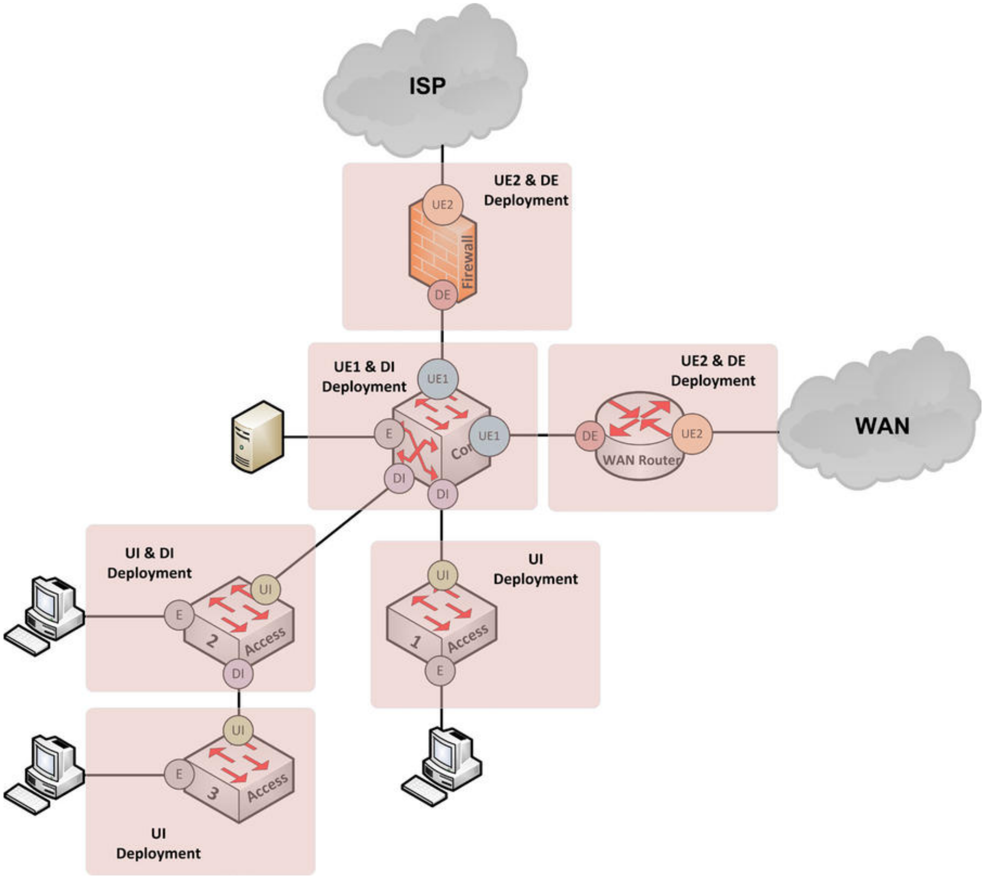
POD: ATT-CON-DEPLOY-UE1



- **When to use**: if the network device will only have an external Uplink port. This will likely be a Collapsed Core switch in a 1-Tier topology.
- **Prerequisites**: --
- **Required**: ATT-CON-BW-UE1-DE, ATT-CON-BW-E (if applicable)
- **Description**: in this deployment, the Core switch (in a 1-Tier topology) would have an external Uplink port connected to either a WAN router, Edge router, and/or Firewall appliance as shown in the picture above.

Example

Continuing with our same topology example, below would be the connection deployment for each device:



- **Firewall**: UE2 and DE Deployment
- **Core Switch**: UE1 and DI Deployment
- **Access Switch #1**: UI Deployment
- **Access Switch #2**: UI and DI Deployment
- **Access Switch #3**: UI Deployment
- **WAN Router**: UE2 and DE Deployment

4.2.2 Bandwidth Services

Determine the bandwidth service for all ports on each network device based on its connection deployment:

	Bandwidth Services for UI Ports	**Bandwidth Services for DI Ports**	**Bandwidth Services for UE2 Ports**
	Bandwidth Services for UE1 & DE Ports	**Bandwidth Services for E Ports**	

Bandwidth Services for UI Ports

POD: ATT-CON-BW-UI

- **When to use**: if the network device has UI port(s)
- **Prerequisites**: ATT-CON-DEPLOY-UI, ATT-CON-DEPLOY-UI-DI
- **Has Sub-PODs**: Go to 4.2.2.1
- **Description**: the bandwidth service for the UI port will be based on the average bandwidth per edge port on the switch. Including edge ports from all switches connected from a DI port (if applicable).

Bandwidth Services for DI Ports

POD: ATT-CON-BW-DI

- **When to use**: if the network device has DI port(s)
- **Prerequisites**: ATT-CON-BW-UI
- **Has Sub-PODs**: Go to 4.2.2.3
- **Description**: the bandwidth service for the DI port must match what exist on the connected device's UI port.

Bandwidth Services for UE2 Ports

POD: ATT-CON-BW-UE2

- **When to use**: if the network device has UE2 port(s)
- **Prerequisites**: ATT-CON-DEPLOY-UE2-DE
- **Has Sub-PODs**: Go to 4.2.2.2
- **Description**: the bandwidth service for the UE2 port will be based on the average bandwidth per user at the site. The bandwidth should consider the number of users and the type of applications/services that will be used.

Bandwidth Services for UE1 and DE Ports

POD: ATT-CON-BW-UE1-DE

- **When to use**: if the network device has UE1 and/or DE port(s)
- **Prerequisites**: ATT-CON-BW-UE2
- **Has Sub-PODs**: Go to 4.2.2.3
- **Description**: the bandwidth service for the UE1/DE port must be within the bandwidth range determined for the UE2 port for the Internet/WAN.

Bandwidth Services for E Ports

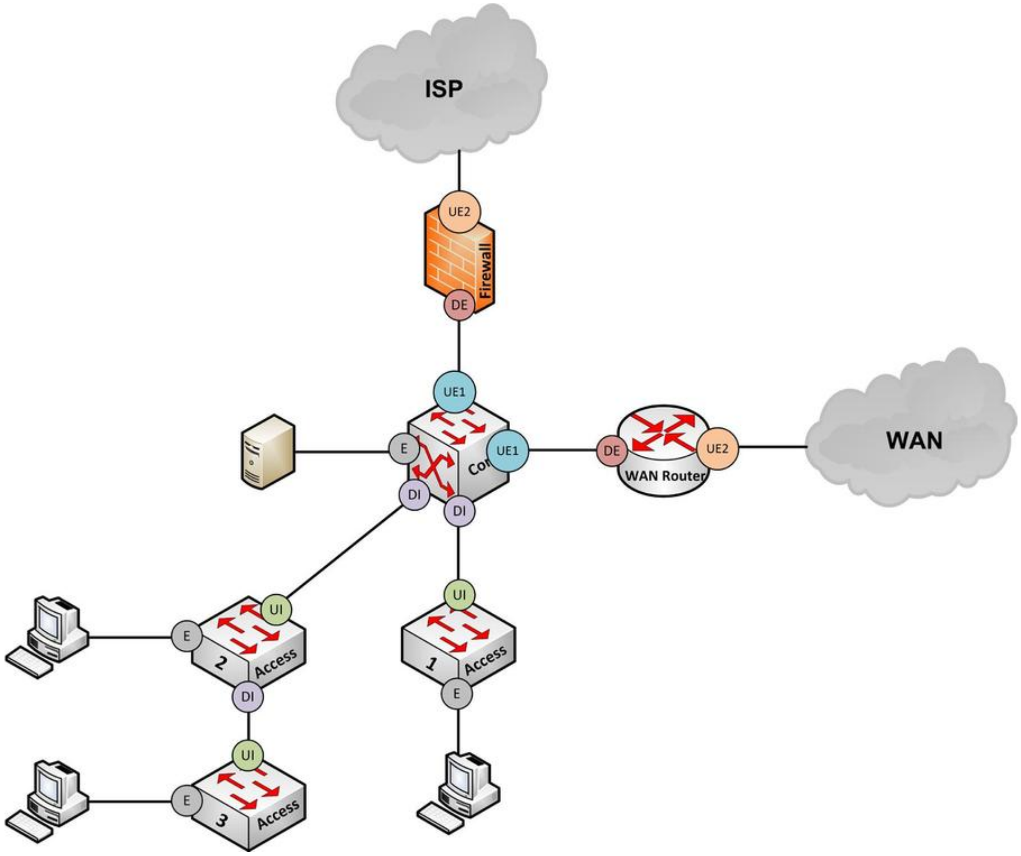
POD: ATT-CON-BW-E

- **When to use**: if the network device has E port(s)
- **Prerequisites**: ATT-CON-BW-UI, ATT-CON-BW-UE1-DE (if applicable)
- **Has Sub-PODs**: Go to 4.2.2.3
- **Description**: the bandwidth service for the E port(s) will be based on the UI port (or UE1 port).

Example

Continuing with our same topology example, we would need to determine the bandwidth service for the ports on each network device in the topology.

- **Bandwidth Services for UI Ports**: Access Switch #1, Access Switch #2, Access Switch #3
- **Bandwidth Services for DI Ports**: Core Switch and Access Switch #2
- **Bandwidth Services for UE2 Ports**: Firewall and WAN router
- **Bandwidth Services for UE1 and DE Ports**: Core Switch, Firewall, and WAN Router
- **Bandwidth Services for E Ports**: Access Switches 1-3, Core Switch



4.2.2.1 Bandwidth Services for UI Ports

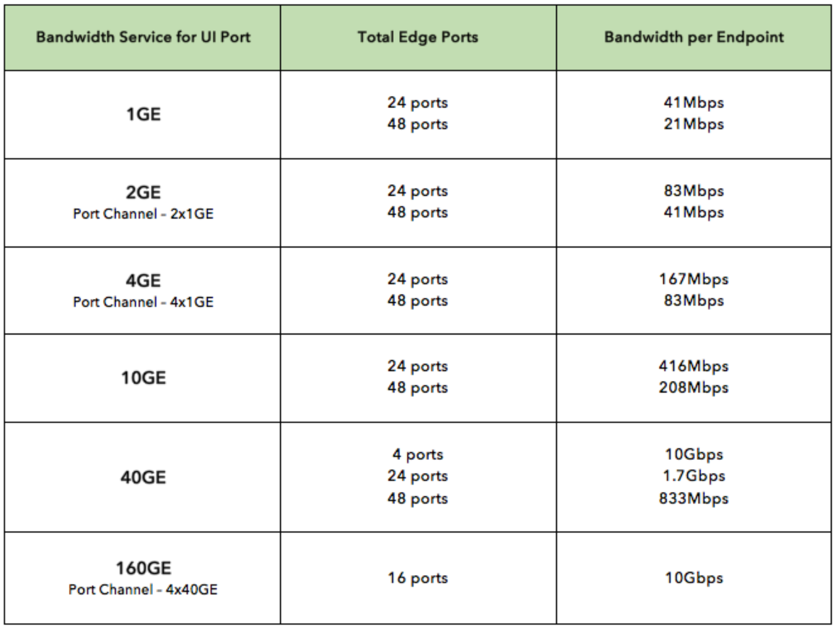
Select one of the following bandwidth services that will be used for the UI ports based on the number of edge ports and the required performance:

Bandwidth Service for UI Port	Total Edge Ports	Bandwidth per Endpoint
1GE	24 ports 48 ports	41Mbps 21Mbps
2GE Port Channel – 2x1GE	24 ports 48 ports	83Mbps 41Mbps
4GE Port Channel – 4x1GE	24 ports 48 ports	167Mbps 83Mbps
10GE	24 ports 48 ports	416Mbps 208Mbps
40GE	4 ports 24 ports 48 ports	10Gbps 1.7Gbps 833Mbps
160GE Port Channel – 4x40GE	16 ports	10Gbps

Note: this chart shows some of the possible combinations and doesn't show the port capacity for a chassis/stack-based switch.

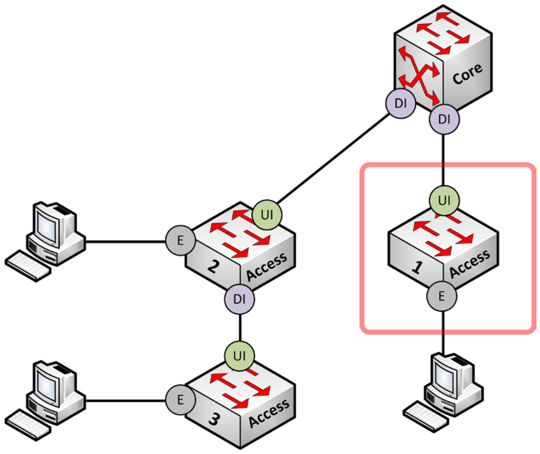
Example

Continuing with our same topology example, we need to determine the bandwidth for all UI ports in the topology. We look at the chart provided in this section. On the left-side column, these are possible bandwidth services we can use for the actual UI port. This port will be based on the number of total edge ports and the average bandwidth per endpoint attached to one of those E ports.



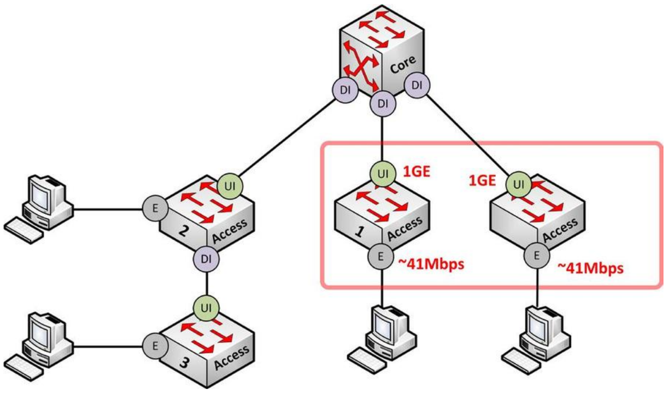
Bandwidth Service for UI Port	Total Edge Ports	Bandwidth per Endpoint
1GE	24 ports 48 ports	41Mbps 21Mbps
2GE Port Channel - 2x1GE	24 ports 48 ports	83Mbps 41Mbps
4GE Port Channel - 4x1GE	24 ports 48 ports	167Mbps 83Mbps
10GE	24 ports 48 ports	416Mbps 208Mbps
40GE	4 ports 24 ports 48 ports	10Gbps 1.7Gbps 833Mbps
160GE Port Channel - 4x40GE	16 ports	10Gbps

Let's start with **Access Switch #1** which has a UI port up to the Core switch. For the UI port, it can be a 1GE, 2GE, up to 40GE. Let's say that the wiring closet, with AS01, will support up to 30 endpoints.

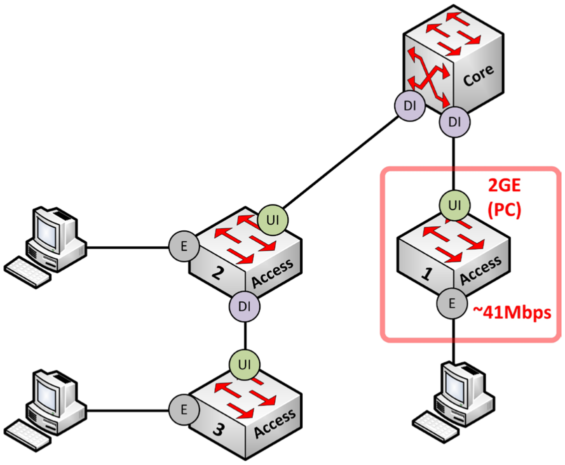


Looking at the chart, if the UI port is a 1GE connection using a 48-port switch, the average bandwidth per user endpoint would be 21Mbps. If that bandwidth is too low then we can consider the following alternatives:

1- Deploying two 24-port access switches in the wiring closet, which would then provide an average bandwidth of 41Mbps per user endpoint.

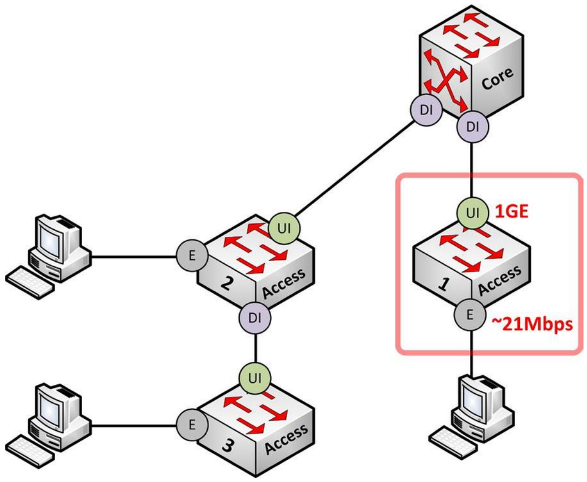


2- Or deploy the UI port as a 2GE connection on the 48-port switch, which would then provide an average bandwidth of 41Mbps per user endpoint.

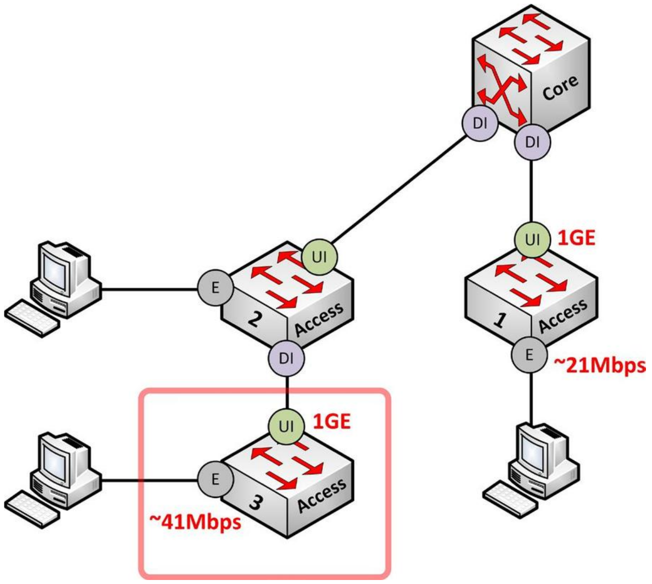


Therefore, you either increase the port speed for the UI port or decrease the total number of edge ports.

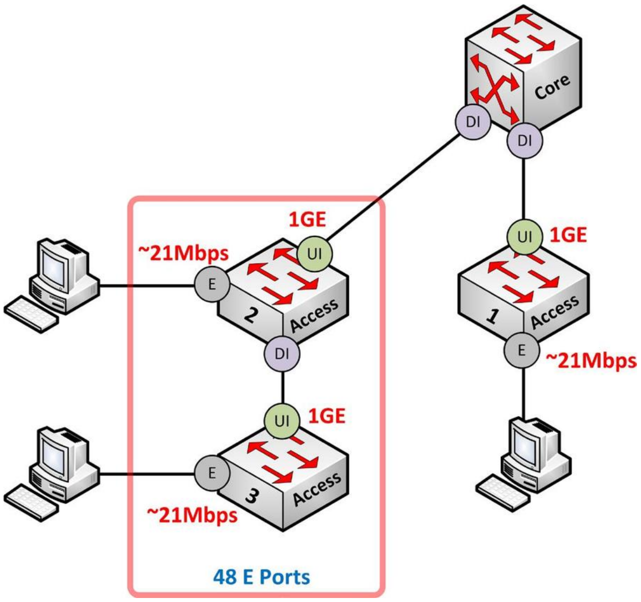
In our example, **Access Switch #1** will have 48-ports and the Uplink will be a 1GE connection supporting an average bandwidth of 21Mbps per endpoint (internally).



For **Access Switch #2**, this will be a little different because this switch has a DI port connecting to another access switch with edge ports. So, let's step back and determine the UI port for Access Switch #3. For **Access Switch #3**, this will be a 24-port switch with a 1GE uplink to Access Switch #2. This would support an average bandwidth of 41Mbps per endpoint. But that will soon change.



For **Access Switch #2**, we need to consider all edge ports locally on the switch plus all edge ports on Access Switch #3 since it is directly connected to it. We will assume that Access Switch #2 will also be a 24-port switch with endpoints attached. This means a total of 48 edge ports between those two switches. If the uplink is a 1GE connection, again, it would provide an average bandwidth of 21Mbps per endpoint. If we want that number to be higher, then again, we can increase the UI port on both switches to maybe 2GE providing 41Mbps per endpoint. We will choose 1GE for all of the uplink connections between those switches.



4.2.2.2 Bandwidth Services for UE2 Ports

In order to determine the bandwidth service for the UE2 port, we need to understand the performance required.

Trying to determine the bandwidth for an Internet (or WAN) connection can be challenging because the traffic conditions cannot be easily calculated starting out. You have to establish a baseline to understand what type of traffic is typically used across your network and the amount of bandwidth utilized. This includes the number of concurrent users that typically access network resources at the same time. Doing all of that can take time which may not be possible for building a new business network with no baseline established.

You can determine the bandwidth using one (or more) of the following methods:

Methods	**Bandwidth Per User Calculation** You can determine the bandwidth by manually calculating what the performance will be based on the traffic services and the type of users that will exist in the environment	**Bandwidth Calculator** You can determine the bandwidth service by using an on-line bandwidth calculator

Bandwidth Per User Calculation

You can determine the bandwidth by manually calculating what the performance will be based on the traffic services and the type of users that will exist in the environment.

The table below will show three main groups based on the bandwidth usage for a user (low, moderate, or high). Each of these groups will list traffic services that can be used based on the user type. You will also see an estimated bandwidth range per user that you can consider for calculating the bandwidth needed for the Internet connection.

User Type	Traffic Services	Bandwidth Per User
Low Performing User	Basic Email Services Basic Web Browsing Services	~90kbps
Moderate Performing User	Basic to Moderate Email Services Basic to Moderate Web Browsing Services Basic File Downloads Cloud Services VoIP Services Streaming Services (Audio, Video)	~130kbps to 256kbps **Note**: If a user will use more than one of the services from the traffic services list, you should consider a higher bandwidth rate within the range provided
High Performing User	Moderate to Heavy Email Services Moderate to Heavy Web Browsing Services Large File Downloads Internet Application Services Web Conferencing Services Cloud Services VoIP Services Streaming Services (Audio, Video)	~256kbps to 512kbps **Note**: If a user will use more than one of the services from the traffic services list, you should consider a higher bandwidth rate within the range provided

Design Consideration: if you are unsure of the number of low, moderate, or high performing users in the environment, you can use 130kbps per user (average baseline). This is typically used to calculate the Internet performance.

Based on the performance calculated, determine the best bandwidth service that should be used for the UE2 port. Use the table below as a reference to make your decision:

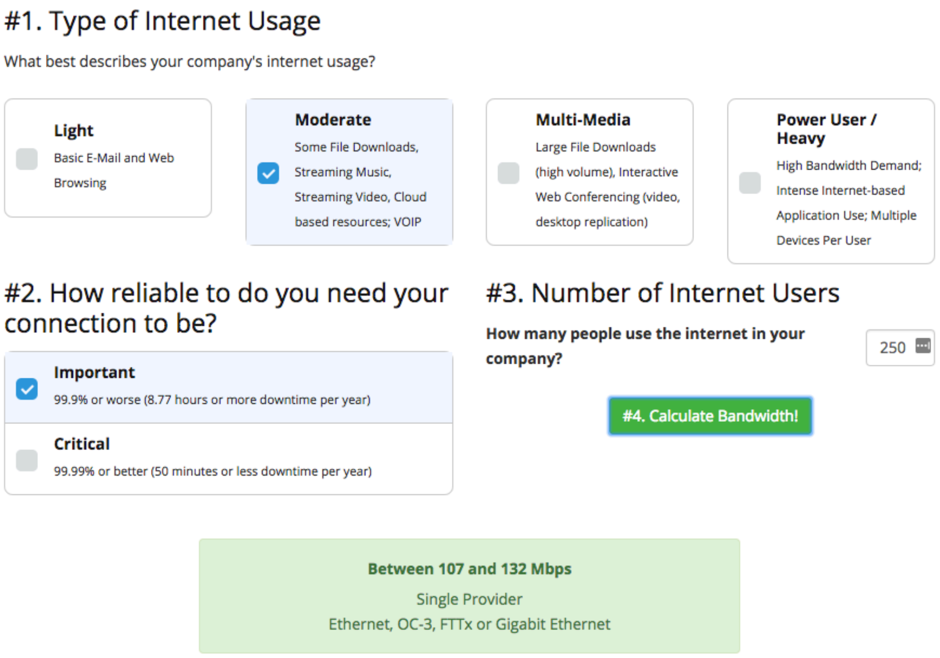
Bandwidth Services	Bandwidth Range	Encapsulations	Notes
T1, E1	1Mbps – 3Mbps	PPP, HDLC, Frame Relay Bundling using MLP, MFR	--
Broadband (DSL, Cable)	10Mbps – 125Mbps	ATM	--
DS-3	45Mbps	ATM	--
Optical (OC)	155Mbps – 9.6Gbps	ATM	--
DWDM	20Gbps – 400Gbps	--	--
Ethernet (FE, GE, 10-GE)	10Mbps – 100Mbps 1Gbps – 100Gbps	VLAN, 802.1Q Bundling using Port Channel	Recommended
Wireless (3G, 4G)	1Mbps – 10Mbps	--	Backup

Bandwidth Calculator

Another alternative to determine the bandwidth service for the UE2 port is using an on-line bandwidth calculator. This does have some risk because the bandwidth calculator that you use will be based on one (or more) mathematical mechanisms. Those mechanisms will vary from tool to tool based on the creator's experience. One specific mechanism may not apply directly with your environment. Therefore, use the information in any bandwidth calculator as a starting point that you can consider for the potential bandwidth service for the UE2 port.

This can be used along with the bandwidth per user calculation method to provide a solid baseline for the bandwidth range that should be considered.

Below is an example for what you can find on-line to calculate the best bandwidth service to use. This bandwidth calculator specifically shows the type of traffic that will be used to even the number of users in the company. You can do a search for "bandwidth calculator" to view several websites that provide these calculations. I'm not listing the URL for this specific bandwidth calculator because it may not be available in the foreseeable future and we are not the owners of that site. A lot of websites come and go over the years creating a lot of dead links in documentation. Therefore, again it is recommended to search for these types of tools on-line.



#1. Type of Internet Usage

What best describes your company's internet usage?

□ **Light** Basic E-Mail and Web Browsing

☑ **Moderate** Some File Downloads, Streaming Music, Streaming Video, Cloud based resources; VOIP

□ **Multi-Media** Large File Downloads (high volume), Interactive Web Conferencing (video, desktop replication)

□ **Power User / Heavy** High Bandwidth Demand; Intense Internet-based Application Use; Multiple Devices Per User

#2. How reliable to do you need your connection to be?

☑ **Important** 99.9% or worse (8.77 hours or more downtime per year)

□ **Critical** 99.99% or better (50 minutes or less downtime per year)

#3. Number of Internet Users

How many people use the internet in your company? 250

Between 107 and 132 Mbps

Single Provider

Ethernet, OC-3, FTTx or Gigabit Ethernet

Example

For the next set of ports, that will be the UE2 ports which exist on the Firewall and WAN router. Here we need to determine the Internet and WAN connection speed up to the service provider. Let's say we have ~140 users (or endpoints) that will access the Internet/WAN. We can do this from two different approaches for calculating the performance required.

- Approach #1: If we don't know how many users are low, moderate, or high performing users, we can consider the average bandwidth of 130Kbps per user. Doing the math that would be 140 users x 130Kbps. That would be ~19Mbps. This means we want to consider a bandwidth technology that can support 19Mbps or higher.
- Approach #2: We can determine the estimated number of low, moderate, and high performing users. Let's say that we will have 100 low performing users that require basic email and web browsing services. And let's say that we will have 40 high performing users.

Since the high performing user type has a recommended range between 256kbps to 512kbps, we need to understand what type of traffic services will be used. Let's say that those high performing users will use the following services:

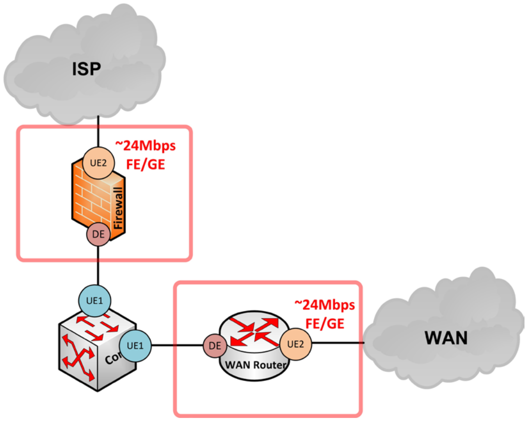
- Moderate to Heavy Email and Web Browsing Services
- Large File Downloads
- Cloud Services

Therefore, let's choose a bandwidth rate that is right in the middle or higher within that range (256kbps to 512kbps). That would be 384kbps, so that is the rate we will use for our high performing users. Doing the math, we will first calculate the two group of users then add the two numbers together:

- 100 users x 90kbps = 9Mbps
- 40 users x 384kbps = 15.3Mbps

9Mbps + 15.3Mbps = **~24Mbps for Internet/WAN Performance needed**.

Therefore, those network devices will have a ~24Mbps connection to the Internet and to the WAN. So, the bandwidth service for those UE2 ports will be FE/GE ports.



4.2.2.3 Bandwidth Services for DI, UE1, DE, and E Ports

Depending on the port type consider the following for the bandwidth service:

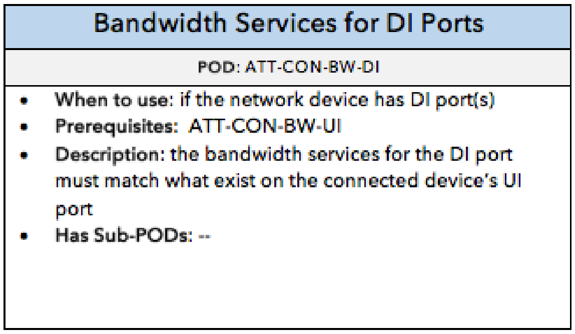
- **UE1 and DE Ports**: the bandwidth service for the UE1/DE port(s) must be within the bandwidth range determined for the UE2 port on the Firewall, Edge router and/or WAN router
- **DI Ports**: the bandwidth service for the DI port(s) must match what exist on the connected device's UI port
- **E Ports on Network Devices with a UI Port Deployment**: the bandwidth service for the E ports will be based on the average bandwidth per endpoint that was determined for the UI port
- **E Ports on Network Devices with a UE1 and DI Port Deployment**: this will likely be a Core switch with one (or more) access switches connected. The bandwidth service for the E ports need to consider intra-communication between the server endpoints locally on the same Core switch. And inter-communication between the user endpoints and the server endpoints.

Below are the bandwidth services that can be used for the DI, UE1, DE, and E ports:

Bandwidth Services	Bandwidth Rate	Additional Notes
Fast Ethernet	100Mbps	--
Gigabit Ethernet	1Gbps	Bundled using Port Channel
10-Gigabit Ethernet	10Gbps	--
40-Gigabit Ethernet	40Gbps	--
100-Gigabit Ethernet	100Gbps	--

Example – DI ports

Moving along to the DI ports, this would apply for our Core switch which is connected down to Access Switches #1 and 2. We also have Access Switch #2 which has an internal downlink port to Access Switch #3. Now in order to determine the bandwidth service for all DI ports, you must have completed the bandwidth service POD for all UI ports which is listed as a prerequisite.



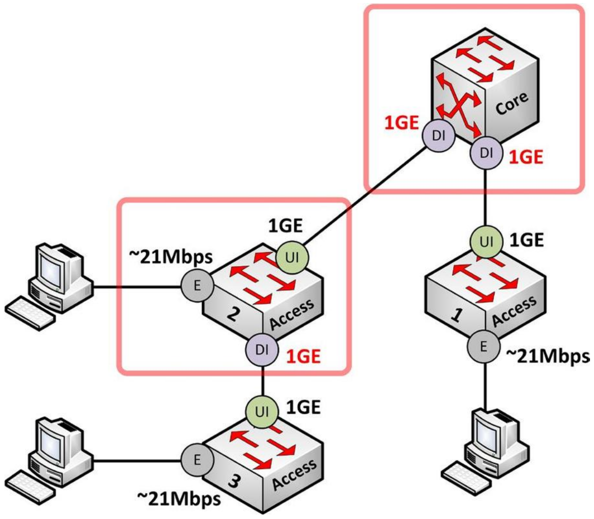
Bandwidth Services for DI Ports

POD: ATT-CON-BW-DI

- **When to use:** if the network device has DI port(s)
- **Prerequisites:** ATT-CON-BW-UI
- **Description:** the bandwidth services for the DI port must match what exist on the connected device's UI port
- **Has Sub-PODs:** --

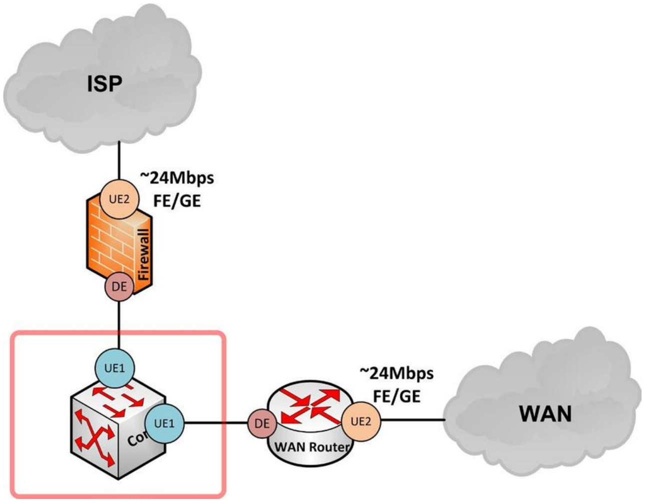
For us, we did complete this POD. For the DI port, this process is very simple. The bandwidth services for the DI port must match what exist on the connected device's UI port.

For the Core Switch, it has a DI port connected to a UI port on Access Switch #1 and #2 which are GE ports. Therefore, the DI ports on the Core switch will also be GE ports matching what is on the other side. For Access Switch #2, it's DI port will also be a GE port matching what exist on Access Switch #3.



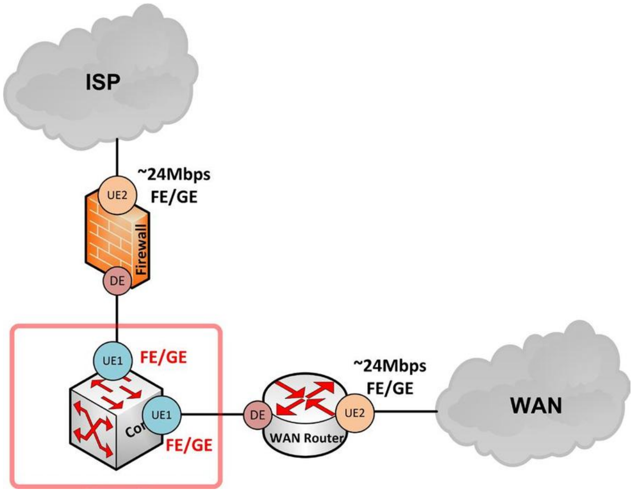
Example – UE1 and DE ports

With the UE2 ports figured out, we can now determine the bandwidth services for the UE1 and DE ports. Starting with the UE1 ports, these types of ports exist on our Core switch which connect to the Firewall and over to the WAN router.

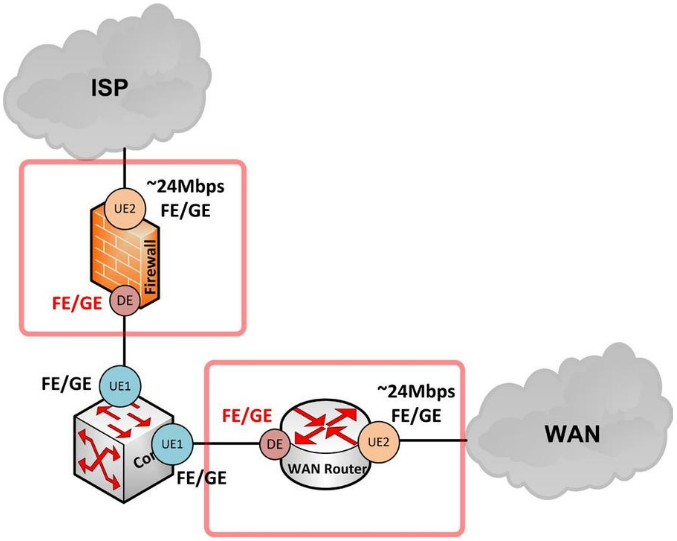


The bandwidth service for the UE1 port must be within the bandwidth range determined for the UE2 port on the Firewall and WAN router. This means, for the Firewall appliance, its UE2 port is 24Mbps using a FE/GE port.

Therefore, the bandwidth service for the UE1 port on the Core must be within the 24Mbps bandwidth range. It will also use a FE/GE port. The same would apply for the UE1 port that connects over to the WAN router.

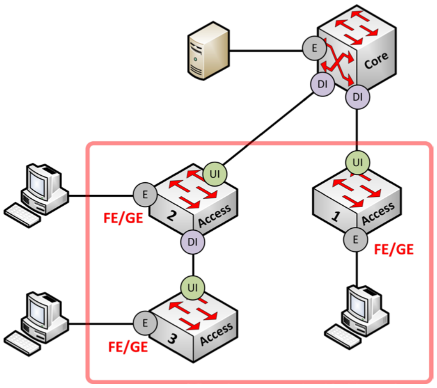


For the DE ports, which exist on the Firewall and WAN router, the bandwidth service must also be within the bandwidth range determined for the UE2 port. Therefore, FE/GE would be used for those ports:



Example – E ports

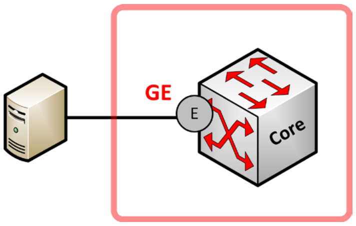
Lastly, we need to determine the bandwidth services that will be used for all E ports. Among all of the access switches, we see the average bandwidth per endpoint that was calculated earlier. Well, we simply need to choose a bandwidth service that is within that range. Since the number is ~21Mbps, we are looking at either FE/GE for the actual E ports on those switches:



Now, for the Core switch, we never determined what the bandwidth average would be since these are likely server endpoints that will be accessed from other endpoints through an uplink port (e.g. access switches). Therefore, there are two considerations we need to keep in mind when it comes to selecting the best bandwidth service for those E ports.

- Intra-communication between the server endpoints locally on the same Core switch
- Inter-communication between the user endpoints and the server endpoints

If there will be servers connected to the Core which will communicate together locally, it’s important to understand the performance requirements. Furthermore, it is also important to understand the number of concurrent users who will access a server that is connected to the Core. For example, we know that the average bandwidth per endpoint for all user E Ports is ~21Mbps, which is based on the UI port speed of 1GE. Let’s say that all endpoints connect to a single server at 21Mbps. This would be an aggregated total of 2Gbps. All endpoints accessing a single server at the same time and at that bandwidth rate is very unlikely, but if it did then the server E-ports would need to be 2GE or 10GE ports. Since that is unlikely especially for user endpoints, we can use GE for the E-ports on the Core switch.



4.3 Networks

Select one (or more) of the following type of networks that will be used in the design:

Networks	**User Network** Dedicated subnets should be used for user endpoints on the LAN which include desktops, laptops, and printers. Multiple user subnets should be considered based on the department, building, or quadrant.	**Guest Network** Dedicated subnet(s) should be used for all guest users and contractors in the environment.
	Server Network Dedicated subnet(s) should be used for all server endpoints which include infrastructure servers, application servers, to database servers.	**Voice Network** Dedicated subnet(s) should be used for all voice endpoints such as IP phones. This is recommended for separating Data and Voice traffic in the environment.
	Management Network Dedicated subnet(s) should be used for managing and monitoring all network devices. Most network devices will have a dedicated management interface which can be configured with a management IP address from this network. This network can also be integrated with an OOB solution for remote administration if the network is not accessible.	**Infrastructure Network** Dedicated subnet(s) should be used for specific network functions and solutions such as Wireless, VPN and WAN.
	Transit Network Dedicated subnet(s) should be used for all point-to-point connections used in the environment.	**Custom Network** Dedicated subnet(s) can be used for a specific purpose defined by the business in the environment.

4.4 Standards

Select one (or more) of the following standards that will be used:

	Naming Standards	**VLAN Standards**	**Addressing Standards**
	Data Center Standards		

Naming Standards

POD: ATT-STD-NAME

- **When to use**: to follow a schema for naming the network devices in the environment
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 4.4.1

VLAN Standards

POD: ATT-STD-VLAN

- **When to use**: to follow a schema for creating VLANs on the network
- **Prerequisites**: SW
- **Required**: --
- **Has Sub-PODs**: Go to 4.4.2

Addressing Standards

POD: ATT-STD-ADDR

- **When to use**: to follow a schema for the IP addressing, prefixes, and subnets used on the network
- **Prerequisites**: --
- **Required**: --
- **Has Sub-PODs**: Go to 4.4.3

Data Center Standards

POD: ATT-STD-DC

- **When to use**: to provide a list of best practices to consider for components in a data center deployment
- **Prerequisites**: ATT-LOC-LOCAL
- **Required**: --
- **Has Sub-PODs**: Go to 4.4.4

4.4.1 Naming Standards

Select one of the following naming standards that will be used for the network devices:

	Standard #1 – Location	**Standard #2 – Client & Hardware**	**Standard #3 – Multi-Site**
	Standard #4 – Client and Location		

Standard #1 – Location

POD: ATT-STD-NAME-1

cs01tra

Core Switch (cs01) located in Tracy, CA (tra)

- **When to use**: this naming standard is ideal for networks located at a single location or sites located in different cities in the same state. This is typically used for small and SMB sized networks

component-deviceID-location

- **Component**: the network device type
- **Device ID**: the network device number. This is important if there are multiple devices on the network
- **Location**: the location or city where the device is located

Standard #2 – Hardware & Client

POD: ATT-STD-NAME-2

asr01rh

Cisco ASR router (asr01) for the client RouteHub (rh)

- **When to use**: this naming standard is ideal for consulting groups that manage network devices for a client. The name will reflect the hardware that is used followed by a unique client ID.

hardware-deviceID-client

- **Hardware**: hardware of the network device using a short acronym
- **Device ID**: the network device number. This is important if there are multiple devices on the network
- **Client**: the client name represented as an acronym

Standard #3 – Multi-Site

POD: ATT-STD-NAME-3

as01-idf1-sc02-ca

Access Switch (as01) in IDF1 (idf1) located in building 2 in Santa Clara (sc02) California (ca)

- **When to use**: this naming standard is ideal for environments that have multiple network devices located in different states, cities, and/or buildings.

component-deviceID-room-location-state

- **Component**: the network device type
- **Device ID**: the network device number. This is important if there are multiple devices on the network
- **Room**: the room (using a room number ID) where the network device is located
- **Location**: the location or city where the device is located
- **State**: the state where the device is located

Standard #4 – Client & Location

POD: ATT-STD-NAME-4

rh-er01-tra-ca

Edge Router (er01) for the client RouteHub (rh) located in Tracy (tra), CA (ca)

- **When to use**: this naming standard is ideal for consulting groups that manage network devices for clients with multiple sites

client-component-deviceID-location-state

- **Client**: the client name represented as an acronym
- **Component**: the network device type
- **Device ID**: the network device number. This is important if there are multiple devices on the network
- **Location**: the location or city where the device is located
- **State**: the state where the device is located

4.4.2 VLAN Standards

Below is a VLAN schema that can be used on the network:

VLAN Schema	**VLAN 10 - 49** Data VLANs (e.g. User Endpoints)	**VLAN 50 - 99** Voice VLANs (e.g. IP Phones)
	VLAN 100 - 149 Internal Server VLANs	**VLAN 150 - 199** External Server VLANs (e.g. DMZ)
	VLAN 200 - 249 Other/Custom VLANs (e.g. Guest, Wireless)	**VLAN 250 - 254** Management and Infrastructure VLANs

This VLAN schema aligned with the IPv4 Addressing schema. For example, VLAN11 (Data VLAN) could have an IP address schema of 192.168.11.0 /24.

This VLAN standard can be used for Small, SMB, Medium, and some Large sized networks.

4.4.3 Addressing Standards

Select one (or more) of the following addressing standards that will be used:

	IPv4 Addressing Standard	**IPv6 Addressing Standard**	

IPv4 Addressing Standard
POD: ATT-STD-ADDR-V4
• **When to use**: if IPv4 addressing will be used on the network • **Prerequisites**: -- • **Has Sub-PODs**: Go to 4.4.3.1

IPv6 Addressing Standard
POD: ATT-STD-ADDR-V6
• **When to use**: if IPv6 addressing will be used on the network • **Prerequisites**: IPV6 • **Has Sub-PODs**: Go to 4.4.3.2

4.4.3.1 IPv4 Addressing Standard

Select one of the following IPv4 addressing schemas that will be used:

🟩	**Schema #1**	**Schema #2**	**Schema #3**

Schema #1

Description: this schema is used for single sites without a WAN

Schema: 192.168 . [Subnet Prefix] . [Host] /24

- [Subnet Prefix] – used to define the network (e.g. User, Voice, Guest)
- [Host] - used for the unique host ID

Example: 192.168.10.101 /24

- 10 = User Network
- 101 = host ID for a user endpoint on that network

Schema #2

Description: this schema is used if there are multiple sites (up to 254 sites) connected to the WAN

Schema: 10 . [Site Code] . [Subnet Prefix] . [Host] /24

- [Site Code] – used to define the site ID for a particular site on the WAN
- [Subnet Prefix] – used to define the network (e.g. User, Voice, Guest)
- [Host] - used for the unique host ID

Example: 10.1.10.101 /24

- 1 = Site #1
- 10 = User Network
- 101 = host ID for a user endpoint on that network

Schema #3

Description: this schema is used if there are multiple sites with up to 15 different type of networks

Schema: 172 . [Subnet Prefix] . [Site Code] . [Host] /24

- [Subnet Prefix] – use values 16 – 31 to define the network (e.g. User, Voice, Guest)
- [Site Code] – used to define the site ID for a particular site on the WAN
- [Host] - this is the unique host ID

Example: 172.17.2.101 /24

- 17 = User Network
- 2 = Site #2
- 101 = host ID for a user endpoint on that network

4.4.3.2 IPv6 Addressing Standard

Select one of the following IPv6 addressing schemas that will be used:

🟩	**Schema #1**	**Schema #2**	**Schema #3**
	Schema #4	**Schema #5**	**Schema #6**

Schema #1

Description: this schema is focused on the location and services for larger networks

Schema: [IPv6 network prefix] [IPv6 subnet prefix = XYZA] [Interface-ID] /64

- [IPv6 network prefix] - this can be a global prefix, unique-local prefix, or site-local prefix
- [IPv6 subnet prefix]
  - X = 4 Bits to define the regional prefix (0-F) ; /52
  - Y = 4 Bits to define the site prefix (0-F) ; /56
  - Z = 4 Bits to define the service/function prefix (Users, Wireless, DMZ) (0-F) ; /60
  - A = 4 Bits to define the subnet ID prefix ; /64
- [Interface-ID] - this is the unique host ID

Example: fd00::1161:aaaa:bbbb:cccc:1

- fd00 = this is a private IPv6 address using a unique-local prefix (fd00::/8)
- 1 = Region #1 (e.g. North America)
- 1 = Site #1 (e.g. San Francisco office)
- 6 = Server network
- 1 = Server network - voice server farm
- aaaa:bbbb:cccc:1 = interface-ID of voice server

Schema #2

Description: this schema is focused on the location based on the country, state, and city which is typical for larger networks

Schema: [IPv6 network prefix] [IPv6 subnet prefix = XYZA] [Interface-ID] /64

- [IPv6 network prefix] - this can be a global prefix, unique-local prefix, or site-local prefix
- [IPv6 subnet prefix]
  - X = 4 Bits to define the country prefix (0-F) ; /52
  - Y = 4 Bits to define the state prefix (0-F) ; /56
  - Z = 4 Bits to define the city prefix (0-F) ; /60
  - A = 4 Bits to define the service/function prefix (Users, Wireless, DMZ) (0-F) ; /64
- [Interface-ID] - this is the unique host ID

Example: fd00::1116:aaaa:bbbb:cccc:1

- fd00 = this is a private IPv6 address using a unique-local prefix (fd00::/8)
- 1 = United States (US)
- 1 = California
- 1 = San Francisco office
- 6 = Voice server network
- aaaa:bbbb:cccc:1 = interface-ID of voice server

Schema #3

Description: this schema is focused on the organization, department, and services

Schema: [IPv6 network prefix] [IPv6 subnet prefix = XYZZ] [Interface-ID] /64

- [IPv6 network prefix] - this can be a global prefix, unique-local prefix, or site-local prefix
- [IPv6 subnet prefix]
  - X = 4 Bits to define the location type (building, site) (0-F) ; /52
  - Y = 4 Bits to define the organization/department prefix (0-F) ; /56
  - ZZ= 8 Bits to define the service/function prefix (Users, Wireless, DMZ) (0-F) ; /64
- [Interface-ID] - this is the unique host ID

Example: fd00::1106:aaaa:bbbb:cccc:1

- fd00 = this is a private IPv6 address using a unique-local prefix (fd00::/8)
- 1 = Building based network
- 1 = Engineering department
- 06 = QA server network
- aaaa:bbbb:cccc:1 = interface-ID of QA server

Schema #4

Description: this schema is focused on the location, organization and services

Schema: [IPv6 network prefix] [IPv6 subnet prefix = XYZZ] [Interface-ID] /64

- [IPv6 network prefix] - this can be a global prefix, unique-local prefix, or site-local prefix
- [IPv6 subnet prefix]
  - X = 4 Bits to define the site code prefix (0-F) ; /52
  - Y = 4 Bits to define the organization/department prefix (0-F) ; /56
  - ZZ = 8 Bits to define the service/function prefix (Users, Wireless, DMZ) (0-F) ; /64
- [Interface-ID] - this is the unique host ID

Example: fd00::1106:aaaa:bbbb:cccc:1

- fd00 = this is a private IPv6 address using a unique-local prefix (fd00::/8)
- 1 = Site #1
- 1 = Engineering department
- 06 = QA server network
- aaaa:bbbb:cccc:1 = interface-ID of QA server

Schema #5

Description: this schema is focused on the services used in smaller networks with multiple sites

Schema: [IPv6 network prefix] [IPv6 subnet prefix = XXZZ] [Interface-ID] /64

- [IPv6 network prefix] - this can be a global prefix, unique-local prefix, or site-local prefix
- [IPv6 subnet prefix]
  - XX = 8 Bits to define the site code prefix (0-F) ; /52
  - ZZ = 8 Bits to define the service/function prefix (Users, Wireless, DMZ) (0-F) ; /64
- [Interface-ID] - this is the unique host ID

Example: fd00::0106:aaaa:bbbb:cccc:1

- fd00 = this is a private IPv6 address using a unique-local prefix (fd00::/8)
- 01 = Site #1
- 06 = Voice server network
- aaaa:bbbb:cccc:1 = interface-ID of voice server

Schema #6

Description: this schema is focused on the services used in smaller networks

Schema: [IPv6 network prefix] [IPv6 subnet prefix = XXXX] [Interface-ID] /64

- [IPv6 network prefix] - this can be a global prefix, unique-local prefix, or site-local prefix
- [IPv6 subnet prefix]
  - XXXX = 16 Bits to define the service/function prefix (Users, Wireless, DMZ) (0-F) ; /64
- [Interface-ID] - this is the unique host ID

Example: fd00::6:aaaa:bbbb:cccc:1

- fd00 = this is a private IPv6 address using a unique-local prefix (fd00::/8)
- 6 = Voice server network
- aaaa:bbbb:cccc:1 = interface-ID of voice server

4.4.4 Data Center Standards

Select one (or more) of the following data center standards that will be used:

	Data Center Facilities	**Data Center - Cooling**	**Data Center - Power**

Data Center Facilities

POD: ATT-STD-DC-FAC

- **When to use**: general data center standards and best practices to consider
- **Prerequisites**: --
- **Has Sub-PODs**: Go to 4.4.4.1

Data Center - Cooling

POD: ATT-STD-DC-COOLING

- **When to use**: data center standards focused on cooling practices
- **Prerequisites**: --
- **Has Sub-PODs**: Go to 4.4.4.2

Data Center - Power

POD: ATT-STD-DC-POWER

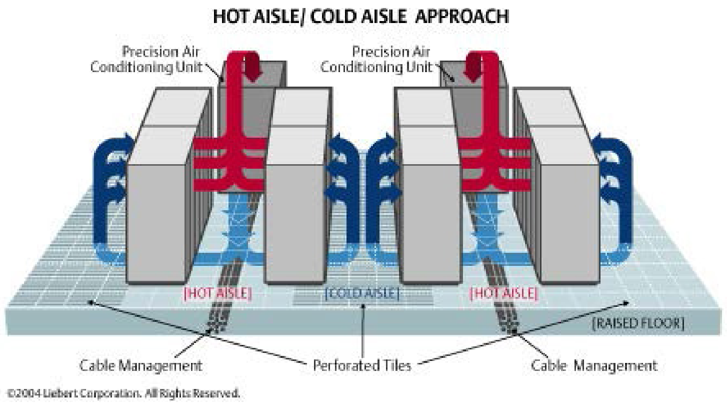
- **When to use**: data center standards focused on power practices
- **Prerequisites**: --
- **Has Sub-PODs**: Go to 4.4.4.3

4.4.4.1 Data Center Facilities

Data center facilities involves environmental (e.g. cooling, air flow, power), management (e.g. cabling, labeling), and equipment (e.g. racks, cabinets, trays) elements. These are really a design in itself, but below are best practice components that should be considered for any data center deployment.

- **Power**: any network equipment (e.g. routers, switches, servers) connecting into a single power circuit should never use more than 75 to 78% of the allocated current (amp) for that circuit as a best practice. For example, if the power circuit is a 20 amp circuit and connected is a power strip with servers, switches, and routers then the equipment's power usage should not exceed 15 amps.
- **Cooling**: it is recommended to ensure proper cooling for the data center so the network equipment do not over-heat and shutdown. Some of the options include: In-row cooling, overhead cooling, raised floor with underfloor cooling, and wall-mounted cooling systems.
- **Racks (or Cabinets):** all equipment (routers, switches, servers, etc.) should be placed into a rack (or cabinet) that is bolted down to the floor and earthquake protected. Determine if a 2-post or 4-post rack will be used. Most Data Center racks will be 4-post racks (42-inch deep cabinets supporting up to ~45RU) which can provide more flexibility for cable and power management.
- **Rack Mounts**: most servers come with rack mounts that use square hole–style vertical cabinet rails. The racks should use the square rail mounting options.
- **Cable Management and Trays**: this should be used for network connections between patch panels and other network devices (e.g. switches). This will provide good cable management and organization in the data center.
- **Labeling**: all devices and cables should be labeled for better management and organization
- **Uninterruptible Power Supply (UPS):** critical network equipment (e.g. Core switch, servers) should be connected to a UPS unit in the event of a power failure. When choosing a UPS system, it's important to determine the following aspects: (1) determine the battery load it can carry and for how long. A UPS system can switchover the current load to a set of internal or external batteries if it is supported. (2) Determine if the UPS system can operate as an on-line system (power is filtered through the batteries all of the time) or a switchable system (the batteries are only used during a power loss).
- **Power Strips**: it's recommended to use Smart or IP enabled power strips that would connect into the network devices. The power strips would then connect into a UPS unit. With IP enabled power strips this can allow engineers to remotely power cycle equipment when needed. Smart Power Strips have the ability to monitor the current Amps that is used for better awareness of the power usage.
- **Temperature**: the temperature in the data center must not be colder than 50 degrees Fahrenheit or hotter than 95 degrees Fahrenheit. It is recommended to keep the data center at an ambient temperature which is between 68 to 77 degrees Fahrenheit.
- **Air Flow**: confirm the airflow for the hardware that will be used. It can be front (intake) to back (exhaust) or right (intake) to left (exhaust), which is NEBS compliant. This is important for cooling and airflow in the Data Center which is discussed further under Hot Aisle and Cold Aisle
    - Use blanking panels to maintain proper airflow for the hardware in a rack/cabinet
    - Use proper vent placement and partitioning of space for the hardware
    - Standalone servers and network chassis (using vertical modules), the air-flow goes front-to-back.
    - For network chassis' (using horizontal modules), the air flow goes left-to-right
- **KVM/ILO (OOB):** this is recommended to provide console access to server equipment if the engineer is unable to access the server directly over the network.
- **Hot Aisle / Cold Aisle**: Use Hot Aisle and Cold Aisles to achieve cooling efficiency. It is important to understand the air flow of the equipment that will be used. You want cool air to flow through the intake of the equipment. Then blowing the hot air out the exhaust and sent through

the AC unit. The picture below provides a best practice for how data center air flow aisles should be used.


HOT AISLE/ COLD AISLE APPROACH
Precision Air Conditioning Unit
Precision Air Conditioning Unit
[HOT AISLE]
[COLD AISLE]
[HOT AISLE]
[RAISED FLOOR]
Cable Management
Perforated Tiles
Cable Management
©2004 Liebert Corporation. All Rights Reserved.

4.4.4.2 Data Center - Cooling

Cooling within your Data Center or any server related room is strongly recommended. Otherwise some of the equipment could shut down if the temperature exceeds 95 degrees for any length of time. The ideal temperature for a server room is typically ~68 degrees. But it's also important to understand that you don't want the Data center to be too cold. Otherwise, that will create a possible condensation problem when the outside air has a high level of humidity leaving moisture on the equipment.

Any electrical component will emit heat, therefore it's important to understand the amount of heat (in Watts) that each device may give off. You also need to consider other related elements that give off heat such as people. People typically give off ~100 watts of heat. Those numbers may be important if you have staff members that work inside of the Data Center for any extended period of time.

To determine the best cooling system needed for the Data Center (or server room) you need to calculate the total wattage for all equipment in that room. Then you factor in the recommended power usage of 75%.

For example, if all of the equipment in the room is 2500 watts. That would be 2500 x 75% which would be 1,875 Watts.

The AC systems will provide cooling power represented in either Tons or BTU (British Thermal Unit):

- **To determine the cooling power based on Tons**: (Total Wattage x 75%) / 3500 = Tons
- **To determine the cooling power based on BTU**: (Total Wattage x 75%) x 3.41 = BTU per hour

Back to our example, we calculated that the total wattage in our Data Center is 1,875 Watts. We can then calculate the cooling power based on Tons or BTU needed in that room.

- **Cooling Power based on Tons**: 1875 watts / 3500 = ~0.54 tons
- **Cooling Power based on BTU**: 1875 watts x 3.41 = ~6394 BTU

Therefore, we can consider a power cooling system that can support those requirements. There is a portal air conditioner unit by KwiKool that supports a cooling power up to 2 tons or 24,000 BTU (picture shown on the right).

Those numbers fall well within our cooling power requirements and recommendations. However, it's always important to factor in scalability for additional equipment added to the Data Center over time.

4.4.4.3 Data Center - Power

It's important to understand the total power (in Watts) that will be used for all network and computer/server equipment. As mentioned earlier, network equipment connecting into a single power circuit should never use more than 75 to 78% of the allocated current (amp) for that circuit. This includes if you are using a UPS for power backup with your critical devices. You can determine the total wattage by calculating the Wattage from all devices. You can typically get this information from the power adapter and/or documentation. You can also calculate the wattage if the voltage and Amps is provided. That formula would be: **Watts = Voltage x Amps**

It's also important to understand what type of power circuits will be used. This will be based on the Voltage and Amps. For example, most dedicated power circuits will be 120v 20amp circuits. The total power wattage for that circuit would be 2400 watts (120 x 20 = 2400). You can take that calculated total and multiple it by 75% which will be 1800 watts (2400 x 75% = 1800). This means as a best practice all network/server equipment plugged into a 120v 20amp circuit should support up to 1800 watts.

Let's say we have a small data center with four servers, two small business switches, and a firewall connected to the Internet. All of these components would be plugged into a single 120v 20amp circuit. The estimated wattage for those devices would be the following:

- Server (250 watts)
- Switch (80 watts)
- Firewall (60 watts)

Doing the math that would be: (4 servers x 250 watts) + (2 switches x 80 watts) + (1 firewall x 60 watts) = 1220 watts

This would be below the recommended usage of 1800 watts for that power circuit. If the number of servers grow over time then a second 120v 20amp power circuit will be required.

This is how you should approach the power design for your Data Center based on the hardware and the power circuits that will be used.

4.5 Resources

Below are the following design resources available in the design cookbook:

	Solution Mappings	Business Size	

4.5.1 Solution Mappings

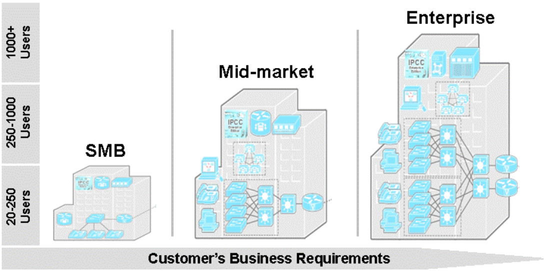
The chart below shows a list of solutions referenced in business/marketing material and what network solutions are actually deployed by the engineer.

For example, a business solution would be something like Collaboration. That isn't a solution by name that would be deployed by an engineer. A network engineer would deploy a Voice or Unified Communication Solution to provide Collaboration to the business.

Business/Marketing Solutions	Actual Network Solutions
Application Delivery Controller (ADC)	Load Balancing
Bring Your Own Device (BYOD)	Wireless – Guest (2.9)
Cloud Computing	Data Center (1.1), Internet (1.4), Computing (2.2.1)
Collaboration	Voice/Unified Communication (2.1.1)
Content Security	Web/URL Security (2.6.5), Mail Security (2.6.13)
Data Loss Prevention (DLP)	Firewall (2.6.2), Mail Security (2.6.8.1), Cloud Security (2.6.12)
Extranet	Internet – DMZ (1.4)
Internet of Everything (IoE)	Data Center (1.1), LAN (1.2), Internet (1.4), Wireless (2.9)
Internet of Things (IoT)	Data Center (1.1), LAN (1.2), Internet (1.4), Wireless (2.9)
Social Networking, Web 2.0	Server Solution
Hyper-Convergence Infrastructure (HCI)	Unified Computing: Hyper-Converged Infrastructure (2.2.2.2)
Remote Office / Branch Office (ROBO)	WAN (1.3)
Mobility	Wireless (2.9)

4.5.2 Business Size

When you choose hardware for the network devices in the topology, it should be aligned to the business size of the environment. The picture below reflects the business size based on the number of users:



Additional Business Sizes: SOHO (up to 10 nodes), Small (10 – 48 nodes)

Understanding the business size is important to provide a baseline when choosing the right hardware for a solution. For example, the Cisco ASA 5506-X firewall is recommended for Small sized networks (around 20-50 users). Therefore, we can start with that model and go up (or down) as needed.

However, the hardware may not align with the business requirements. For example, a Microsoft Gold Partner with 30 employees was looking for a new phone system. Based on the business size they would be an SMB sized network. The Cisco Unified Communication Manager Express (CME) solution would easily support this client based on their business size. However, they had unique SIP requirements that wasn't supported on Cisco Unified CME (at the time), so we deployed the Cisco Unified Communications Manager solution (suited for larger networks) to meet their technical requirements.

Keep these considerations in mind for all hardware selections in the environment.