

What's New in NSX-T 3.1.1

Nicolas MICHEL
NSBU PM/TPM Team

February 2021

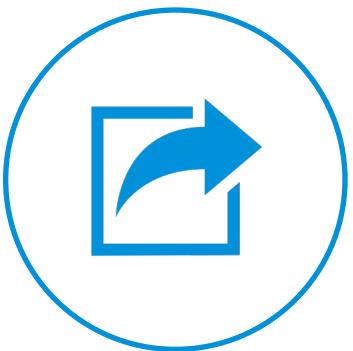
Introducing NSX-T 3.1.1

Maintenance Release with OSPF support



Cloud Scale Networking

- OSPFv2 Support
- Federation Scale enhancements
- DHCP4 relay support on Service Interface



V2T Migration

- Lift and Shift in UI
- Two options for in-place
- Support VCF
- Support vRA enhancements(*8.3)
- Support Universal Objects in one site



Platform Enhancements

- N-vDS to VDS migration
- NSX-T Local Users (RBAC) Support
- NSX-T ALB Policy API Support
- NSX-T Identity Firewall Configuration Policy API
- VDS Licensing for NSX users



NSX Cloud

- NSX Manager in Azure Marketplace
- Horizon Cloud integration
- AWS TGW support for Security use-case



What's New in NSX-T 3.1.1

Federation

PM: Jerome Catrouillet

TPM: Dimitri Desmidt

February 2021



Scale

- Increase of # of Hypervisors from 256 to 650.



Orchestration

- Orchestration using PowerCLI

Examples of Terraform and PowerCLI on:

<https://github.com/vmware-samples/nsx-t/tree/master/helper-scripts/Multi-Location/Federation/End2End>



What's New in NSX-T 3.1.1

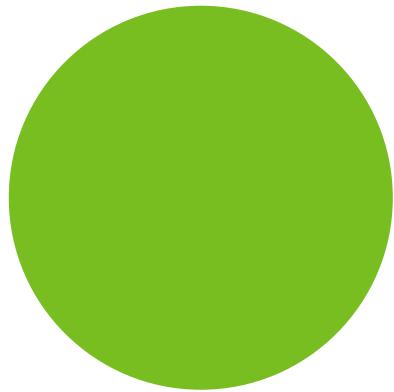
NSX Cloud

PM: Shiva Somasundaram

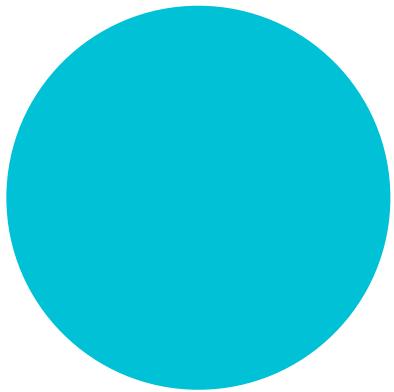
TPM: Geoff Wilmington

February 2021

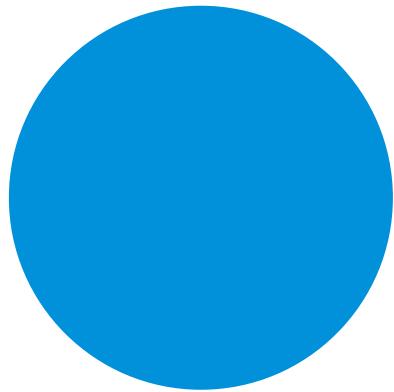
Updates and Improvements



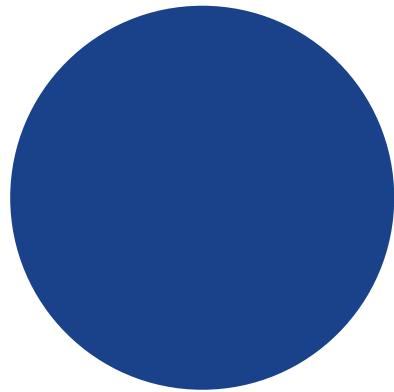
NSX Manager and
Control Plane in Azure
via Azure Marketplace



Horizon Cloud Day-0
Installation and
Coordination

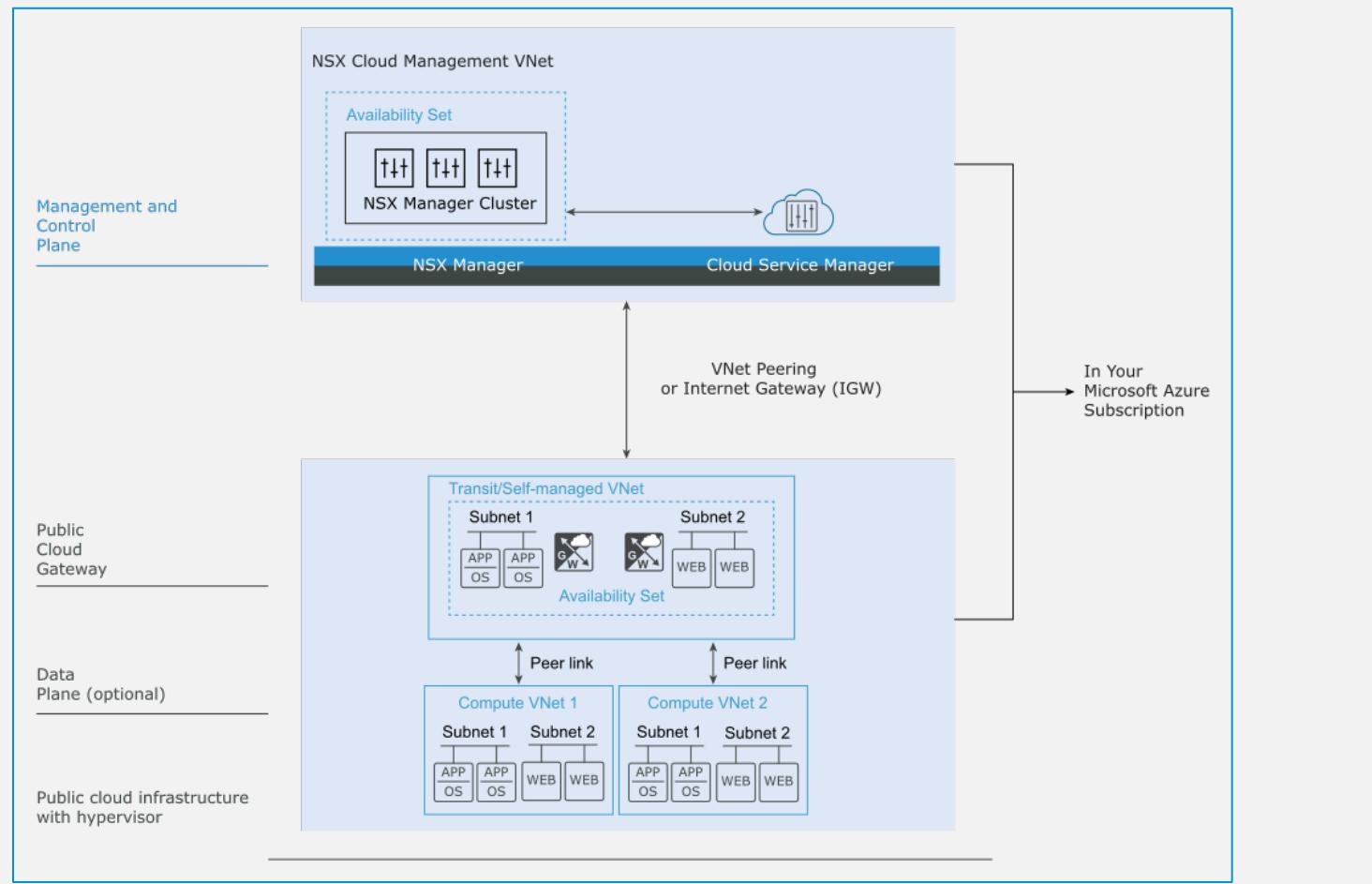


Support for PCG &
AWS TGW



CSM Resiliency and UI
Improvements

NSX Manager and Control Plane in Azure via Azure Marketplace and Terraform



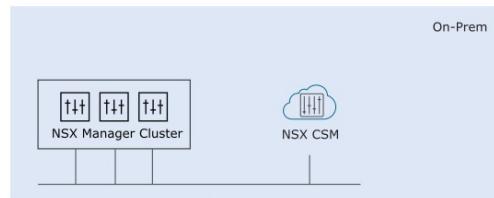
Deployment of NSX Manager and CSM directly into an Azure VNet using Terraform Provider

- Azure Marketplace and Terraform provider will be available after Azure VHD submission approvals

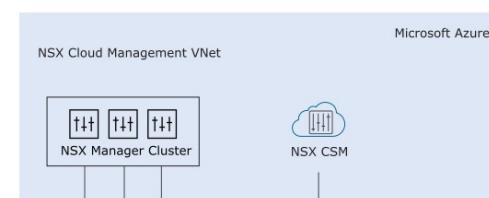
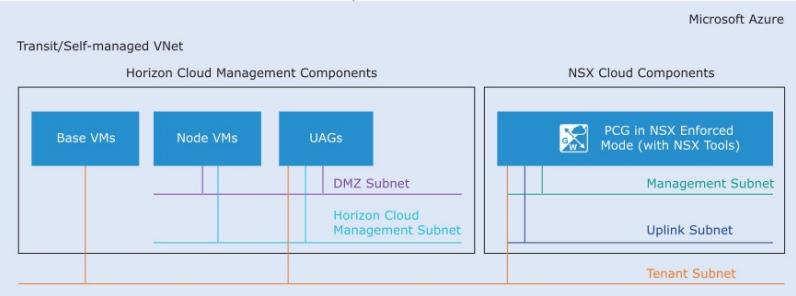
No on-premises NSX-T presence required

- *Federation not supported

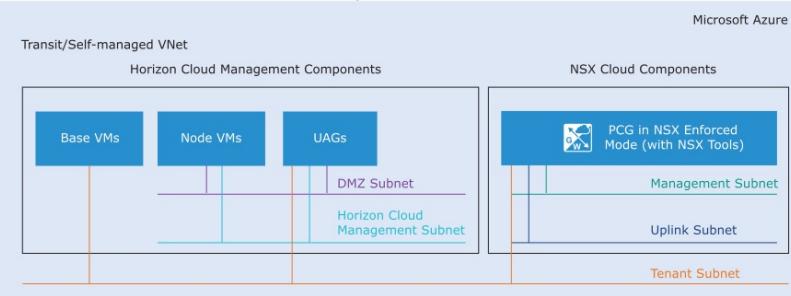
Horizon Cloud Day-0 Installation and Coordination



Express Route/Direct Connect
or Site to Site VPN over internet
or over Internet Gateway (IGW)



Peered Connection
or Internet Gateway (IGW)



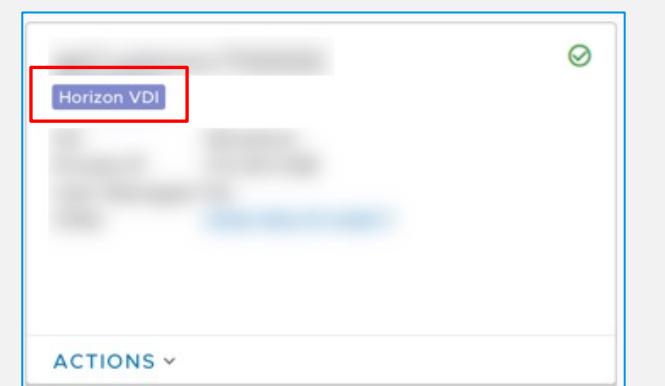
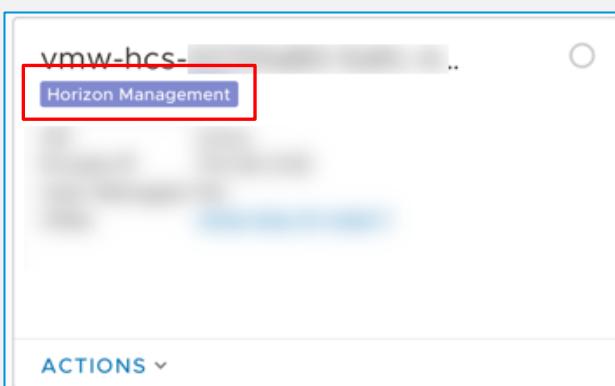
Supported for NSX Manager deployed in Azure or on-premises

- Native Azure NSX deployment

NSX Tools can be automatically installed into the base image

NSX Cloud differentiates HCS on Azure Components

Auto-created security policies for Horizon Cloud components and VDI machines





What's New in NSX-T 3.1.1

Platform Security

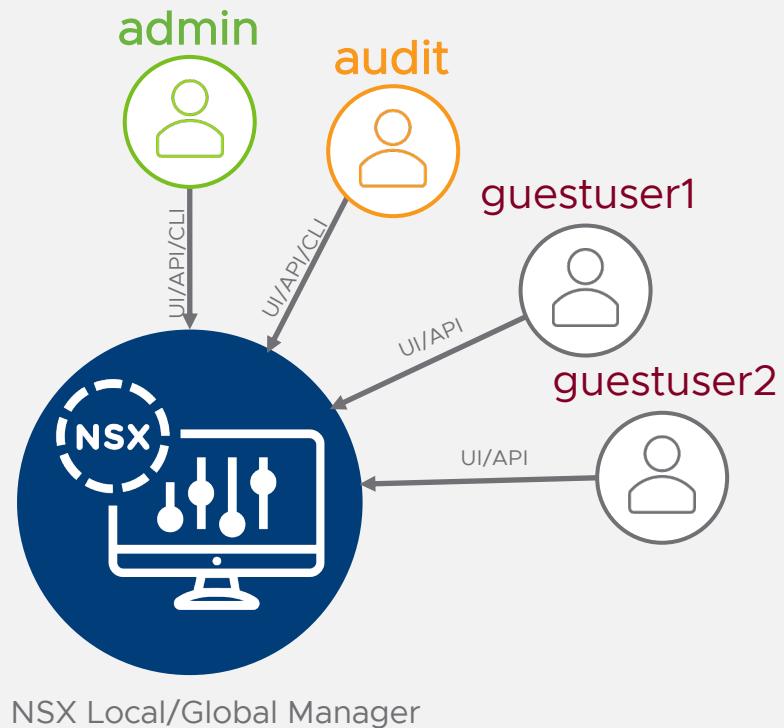
PM: Rajiv Prithvi
TPM: Ganapathi Bhat

February 2021

Platform - Security

NSX-T "Local" Users - Overview

NSX-T 3.1.1



Overview

- NSX has following system created Local users on both Local Manager and Global Manager:
 - admin -> UI/API/CLI
 - audit-> UI/API/CLI
 - guestuser1-> UI/API
 - guestuser2 -> UI/API
 - root* -> CLI`
- By default, local users audit, guestuser1 & guestuser2 are inactive
- Cannot add/delete local users, but can be renamed
- RBAC role can be changed only to "guestuser1 & guestuser2" , default "auditor" (network admin/security admin)
- Option to add remote users using LDAP/VIDM** integration with different RBAC role
- With NSX Manager cluster, Resetting local user password on one automatically sync's that to other nodes in the cluster

*-> Shell User-Mainly for advanced level of debugging with VMware support only.
**-> As of 3.1.X - NSX Global Manager supports only VIDM .

Platform - Security

UI Page for Users & RBAC Roles

NSX-T 3.1.1

Home | Networking | Security | Inventory | Plan & Troubleshoot | System

User Role Assignment | Local Users | Roles | LDAP | VMware Identity Manager

Users and Roles

	User Name	User ID	Status
	admin	10000	Active
	audit	10002	Not Activated
	guestuser2	10004	Not Activated
	guestuser1	10003	Not Activated

2 New Local users in 3.1.1

Edit | Activate User

Home | Networking | Security | Inventory | Plan & Troubleshoot | System

User Role Assignment | Local Users | Roles | LDAP | VMware Identity Manager

Users and Roles

	User Name	User ID	Status
	admin	10000	Active
	audit	10002	Not Activated
	guestuser1	10003	Not Activated
	changetoyourname	10004	Active

Guestuser2 is renamed and activated with password.

Home | Networking | Security | Inventory | Plan & Troubleshoot | System

User Role Assignment | Local Users | Roles | LDAP | VMware Identity Manager

Users and Roles

User/User Group Name | Roles | Type

User/User Group Name	Roles	Type
admin	Enterprise Admin	Local User
changetoyourname	Auditor	Local User
guestuser1	Enterprise Admin	Local User

New Local Users can have ANY RBAC role (default auditor)

SAVE | CANCEL | Select Roles

Enterprise Admin
GI Partner Admin
LB Admin
LB Operator

Home | Networking | Security | Inventory | Plan & Troubleshoot | System

User Role Assignment | Local Users | Roles | LDAP | VMware Identity Manager

Users and Roles

	User Name	User ID	Status
	admin	10000	Active
	audit	10002	Active
	guestuser1	10003	Active
	changetoyourname	10004	Active

User with Enterprise Admin RBAC role can reset local user password

Edit | Deactivate User | Reset Password



What's New in NSX-T 3.1.1 OSPF

PM: Jerome Catrouillet

TPM: Nicolas Michel

February 2021

OSPF

OSPF Generalities

NSX-T 3.1.1 supports **OSPFv2** described in [RFC2328](#).

Open Shortest Path First is a **link state routing protocol** and is considered as an **IGP**.

IGP (Interior Gateway Protocol): Advertise routes within an Autonomous System.(OSPF, RIP, IS-IS, EIGRP)

EGP (Exterior Gateway Protocol): Advertise routes between Autonomous Systems. eBGP is the only EGP nowadays.

OSPF is a link state routing protocol based on the Dijkstra Shortest Path First Algorithm to compute routes.

- Distance Vector routing protocol: Advertise the best path (metric or distance) to all neighbors.
- Link State routing protocol: Advertise links information (status) into a database (LSDB) and compute a map of the network. Support network hierarchies (areas). Converge faster than Distance Vector and scales better.



OSPF

OSPF Generalities - Operations

1 - Build Adjacency:

- OSPF enabled routers try to establish an adjacency by sending "Hello" packets. Adjacency is established if parameters match between the routers. (Timers/Subnet mask/MTU etc..)

2 - LSA flooding:

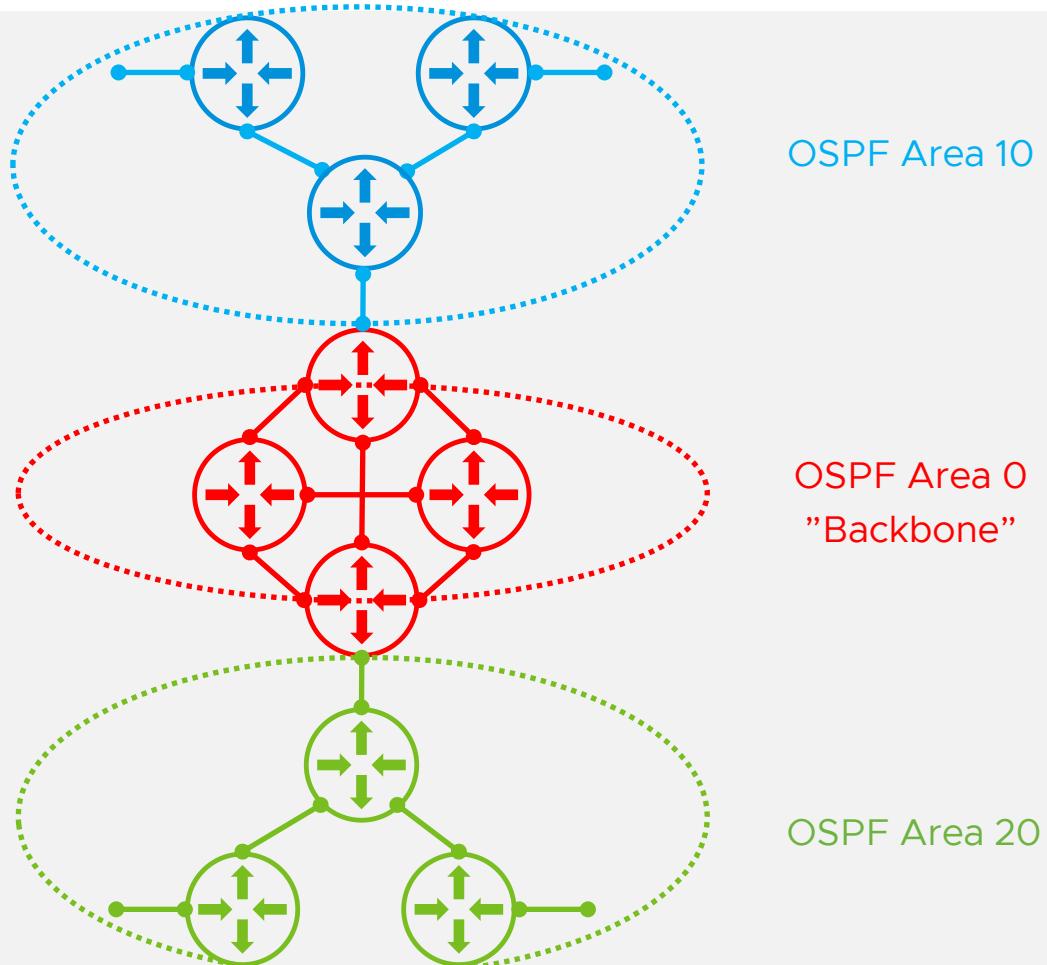
- Link state advertisement are information regarding links/interfaces and their status. These LSA are flooded router to router within an area. Multiple types of LSA: Router - Network – Summary – Summary ASBR – External – Multicast – NSSA etc ...
- These LSAs are injected into a Link State Database.
- To optimize LSA flooding, OSPF elects a Designated Router ([DR](#)) and Backup Designated Router ([BDR](#)) using priority. [A Tier-0 gateway will never be elected DR/BDR \(priority 0\)](#)

3 – Dijkstra Computation and routing table processing:

- Each router will create a map of the networking topology based on the LSA flooded previously (Shortest Path to each destination).

OSPF

OSPF and Areas



OSPF Routers in an Area have the same detailed topology for their own area only. (no detailed knowledge of the topology of another area to reduce CPU burden).

An OSPF router can have links in different areas (ABR). **NSX-T supports 1 Area per gateway (no ABR functionality).**

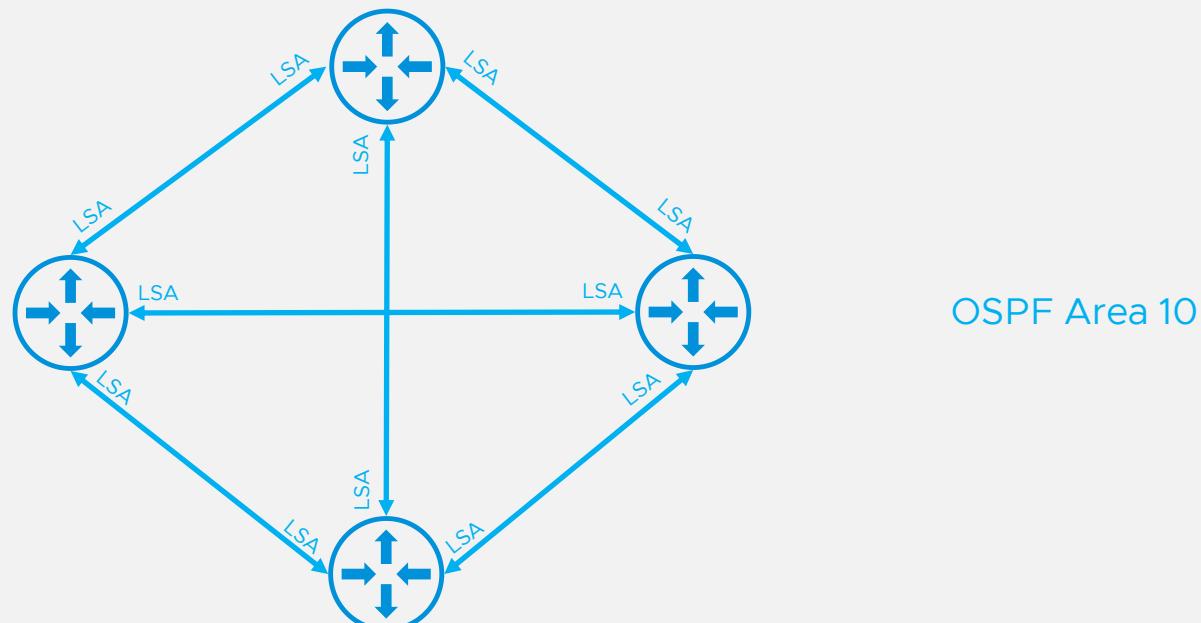
A link can be in only one area

OSPF routers in area 10 only needs to know how to exit their area.

Area 0 exchanges the routing information to other areas

OSPF

OSPF and Areas

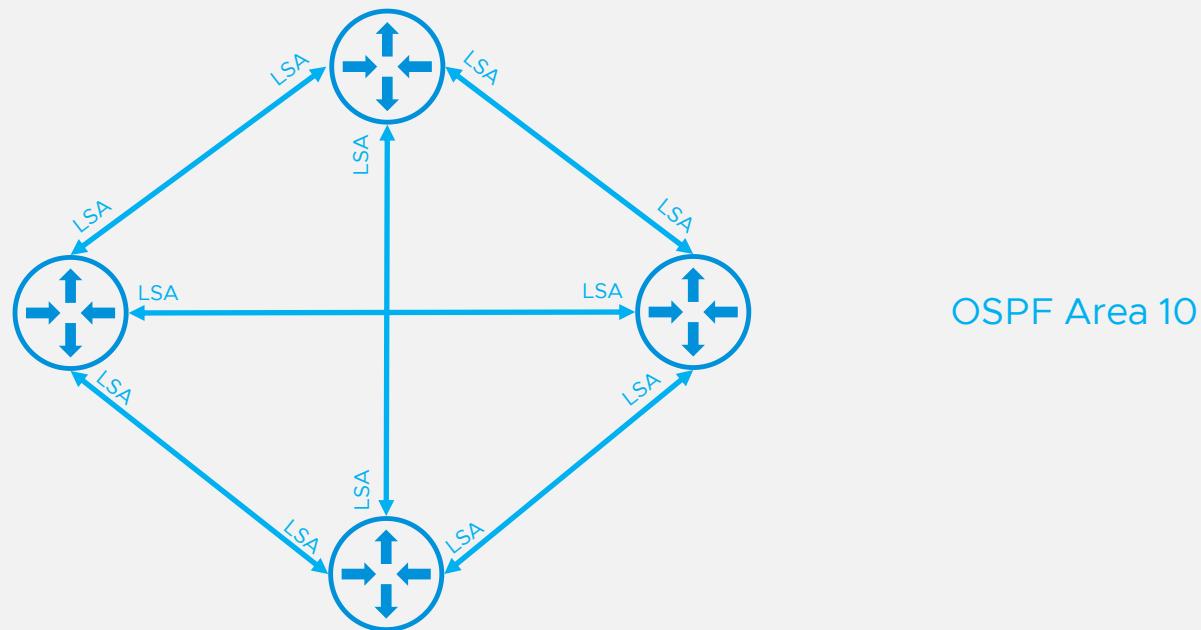


After an Adjacency has been established, **OSPF Routers will flood LSAs** (Link State Advertisement) to all OSPF neighbors. There are multiple types of LSAs :

- Type 1: Router LSA (Interfaces - neighbors)
- Type 2: Transit subnets for Broadcast network (not used in P2P)
- Type 3: Summary LSA. LSA sent from an ABR inside an Area
- Type 4: ASBR LSA
- Type 5: External LSA
- Type 7: NSSA

OSPF

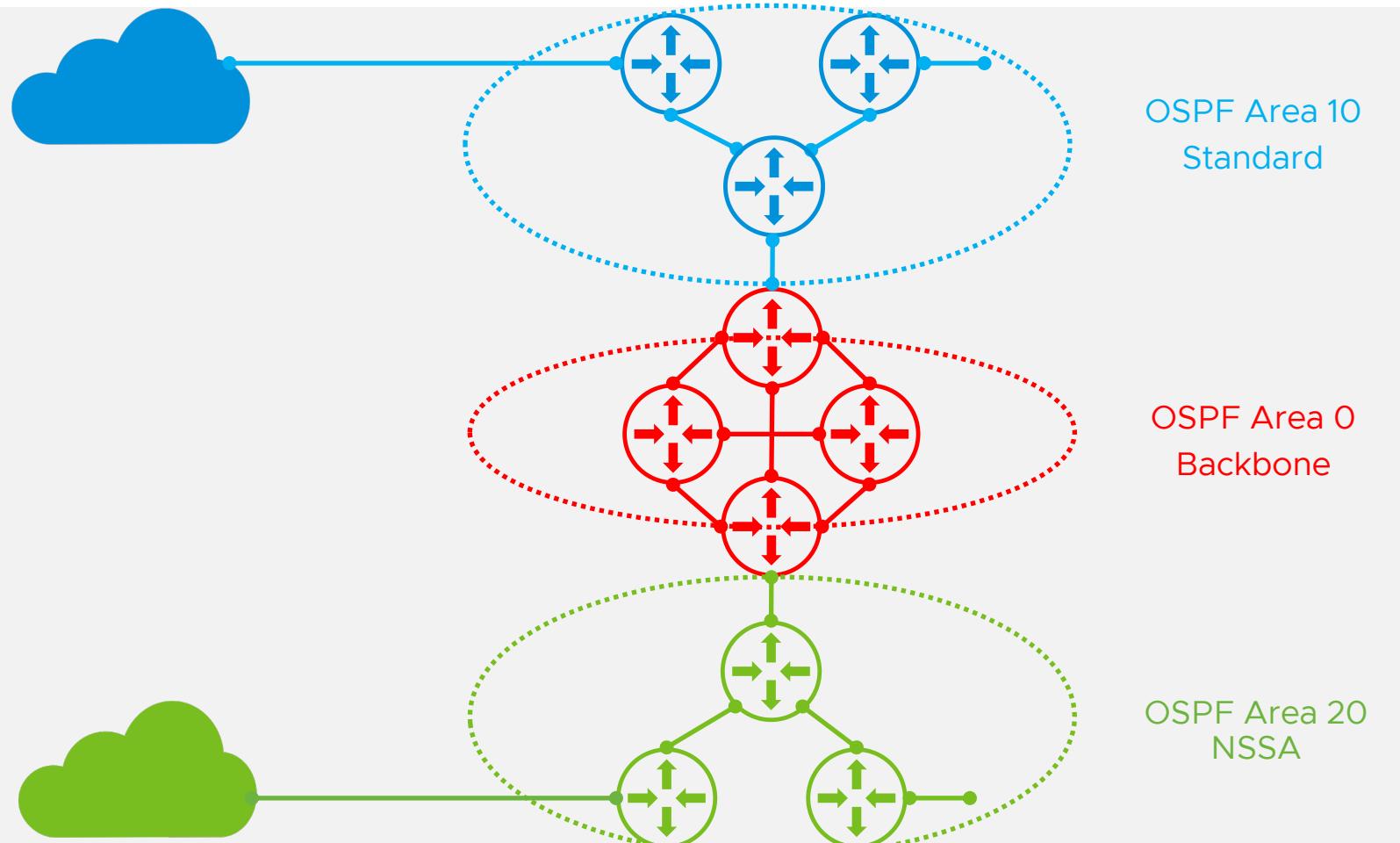
OSPF and Areas



LSA Database must be **identical** for each node in the area.

Each Router will compute a map of the topology in the area.

When a link fails, the router will flood its LSAs to **all OSPF routers** in the area which will trigger another Dijkstra computation



Standard Area: Non backbone area that needs to be connected to a backbone area (OSPF area 10) using an ABR (Area Border Router). External LSA (type 5) can be injected in that kind of area.

Backbone Area: Must be design with redundancy in mind and cannot be partitioned. Has knowledge of the entire topology. Inter Area Traffic must flow through it.

Not so Stubby Area: Does not allow “External LSA” (Type 5) to be injected but will rather use “Not so Stubby” LSA (Type 7). Routes will be advertised into OSPF as ”N2” instead of “E2”. Lower the amount of LSAs (no Type 5 LSA. Instead, a Default is injected into the Area). **Use for scale**

Virtual links are not supported.

OSPF Adjacencies

Before sending LSAs in an OSPF area, a router needs to establish an adjacency with another OSPF peer. Adjacencies are established using “hello” packets.

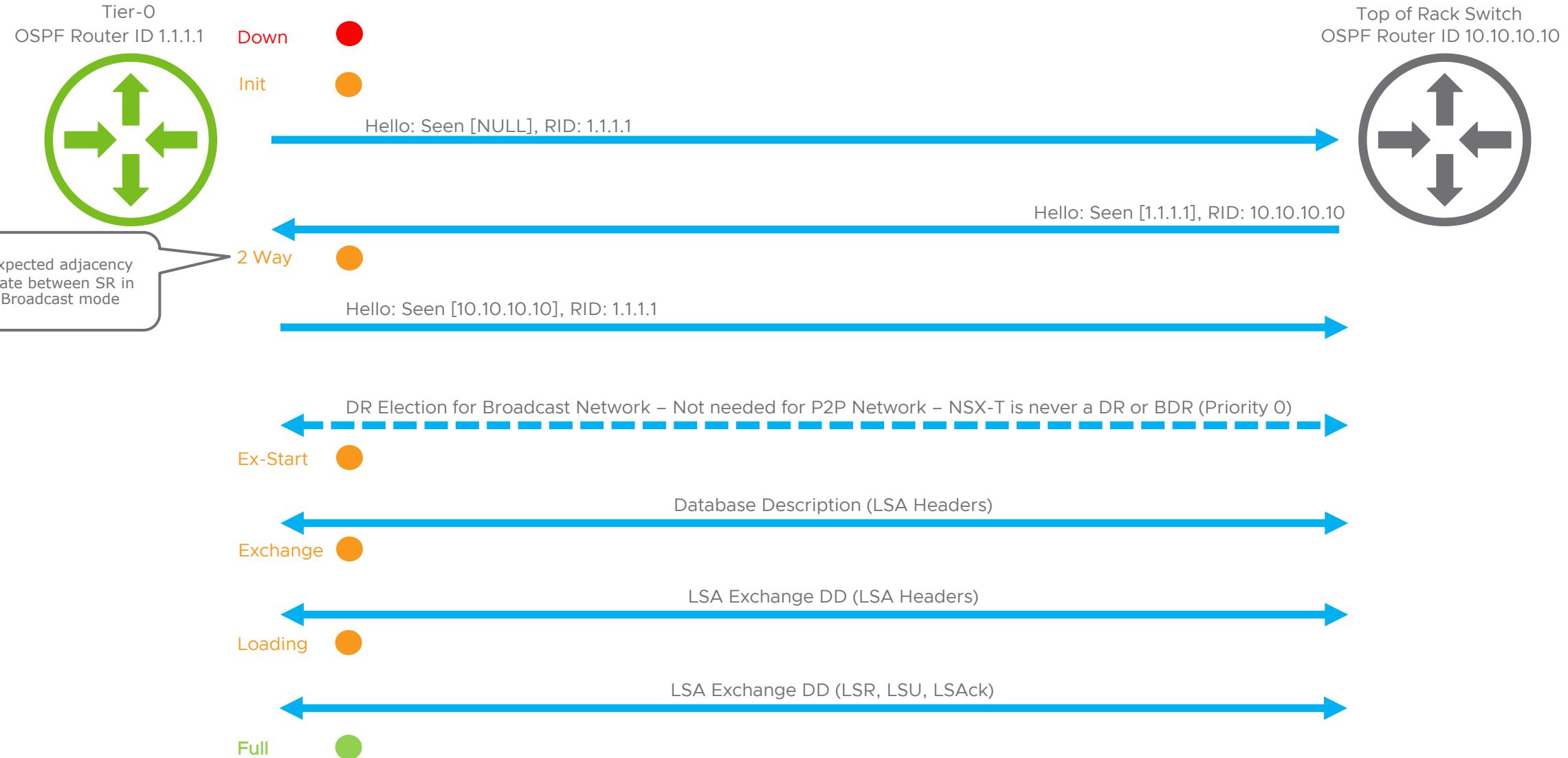
An OSPF router identifies itself within the area using a unique ID: “router-id”. In NSX-T 3.1.1, the OSPF router-id is inherited from BGP when an interface is configured on a Tier-0. **(Behavior currently discussed between Engineering and PM/TPM)**.

Some Parameters in the Hello packets (Dst IP: 224.0.0.5 – All SPF Routers) must match between OSPF peers to establish a proper and healthy adjacency:

- Area
- Subnet Mask configured on that interface
- MTU
- OSPF Timers (Hello / Dead)
- Interface Type (P2P / Broadcast ...)
- Router Priority
- Unique Router-ID

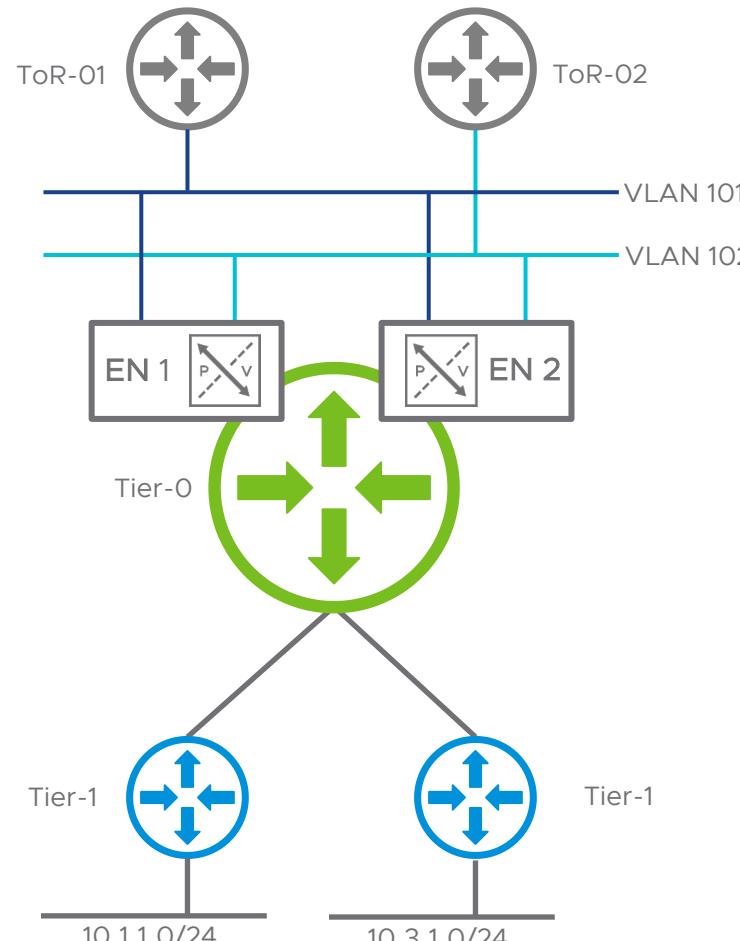


OSPF Adjacencies

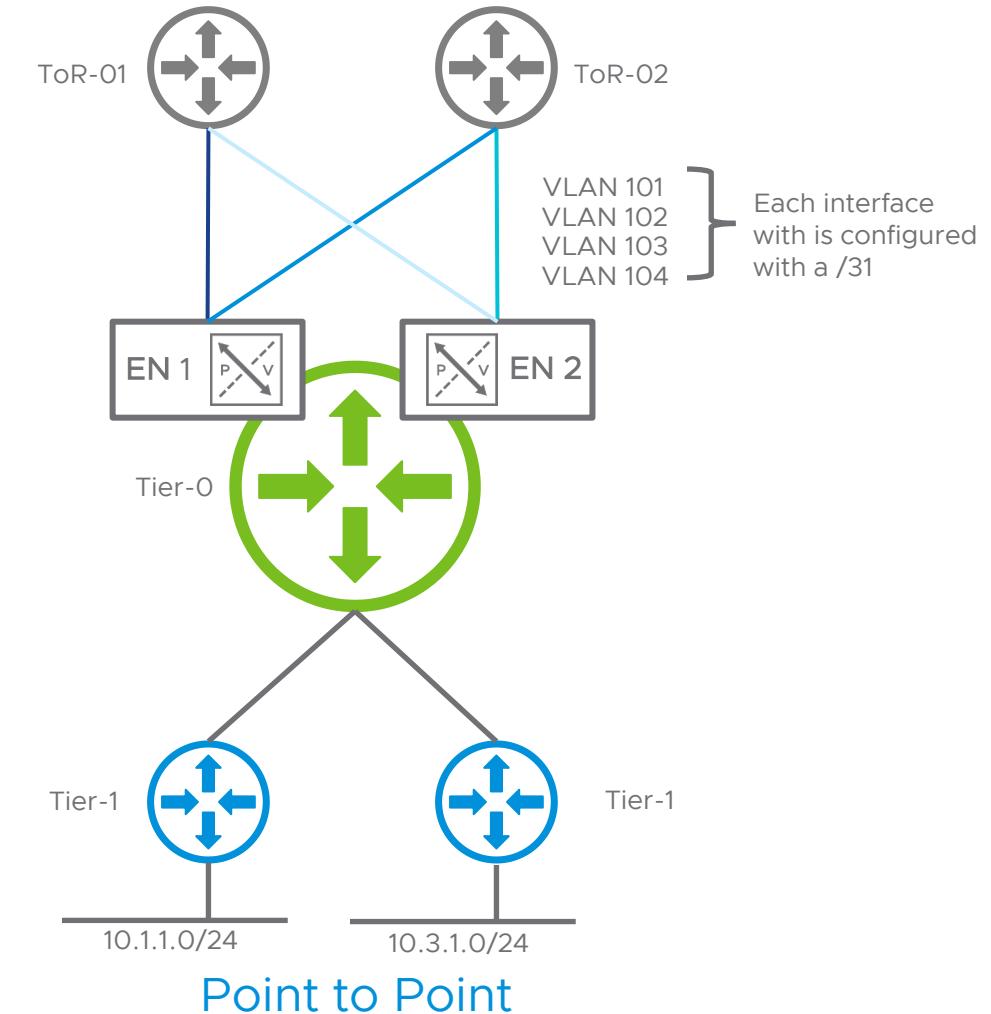


OSPF Adjacencies

NSX-T 3.1.1 support interfaces to be configured as **Point to Point** or **Broadcast** for OSPF



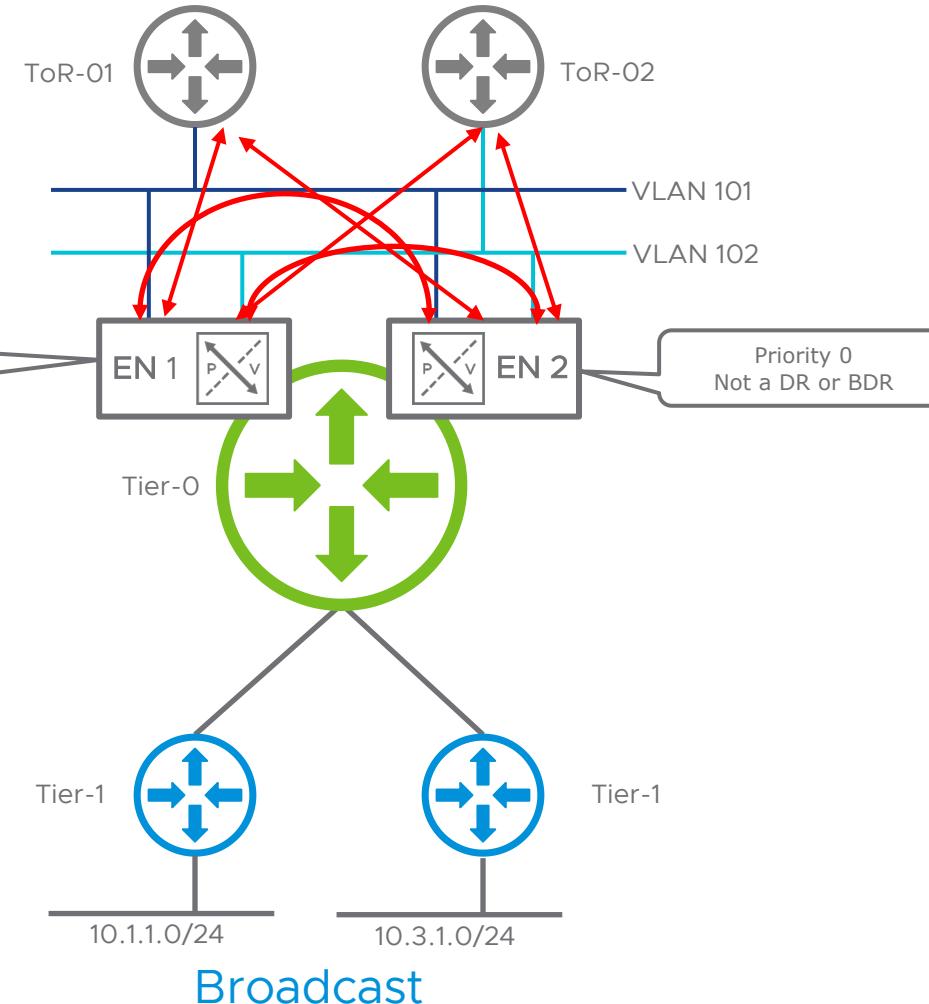
Broadcast



Point to Point

OSPF Adjacencies – Broadcast

NSX-T 3.1.1 support interfaces to be configured as **Broadcast**.

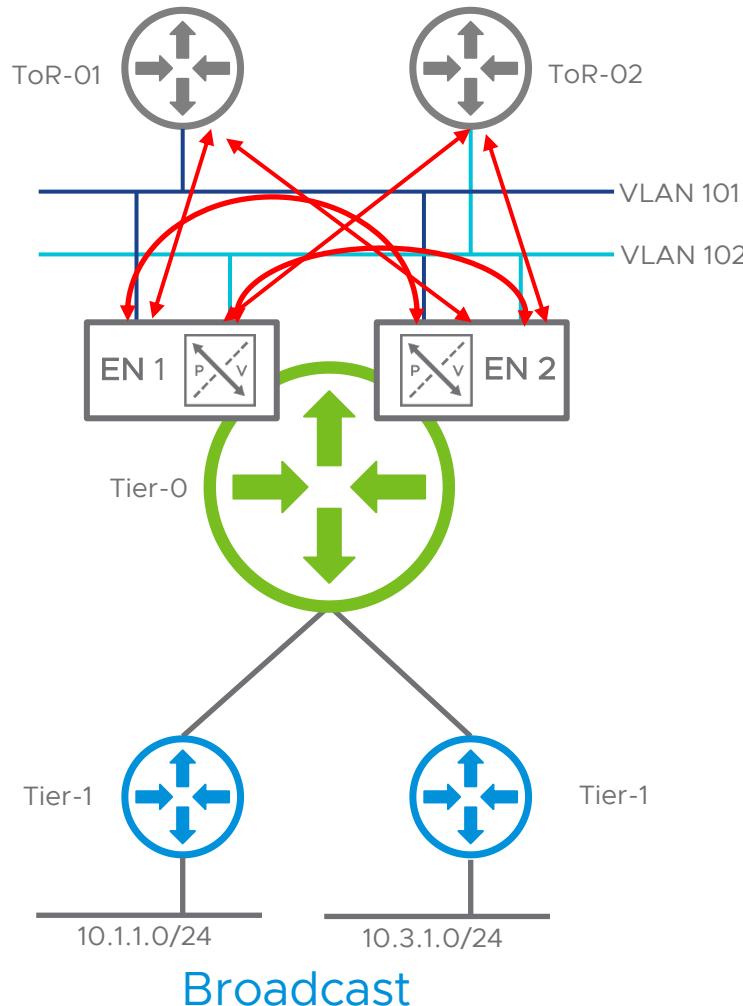


DR/BDR election: NSX-T **Priority=0**

OSPF Neighbors						
Tier-0 Gateway	Tier0-Tenant...	#Neighbors				
Last Updated On: Feb 1, 2021, 4:21:03 PM						
Neighbor IP Address	Interface	Source	Edge Node	Priority	State	
> 10.10.10.10	uplink-326:172.16.10.2	172.16.10.10	EDGE-02	1	Full	
> 11.11.11.11	uplink-328:172.16.11.2	172.16.11.11	EDGE-02	1	Full	
> 172.16.11.1	uplink-326:172.16.10.2	172.16.10.1	EDGE-02	0	2-Way	
> 172.16.11.1	uplink-328:172.16.11.2	172.16.11.1	EDGE-02	0	2-Way	
> 10.10.10.10	uplink-323:172.16.10.1	172.16.10.10	EDGE-01	1	Full	
> 2.2.2.2	uplink-288:172.16.11.1	172.16.11.2	EDGE-01	0	2-Way	
> 2.2.2.2	uplink-323:172.16.10.1	172.16.10.2	EDGE-01	0	2-Way	
> 11.11.11.11	uplink-288:172.16.11.1	172.16.11.11	EDGE-01	1	Full	

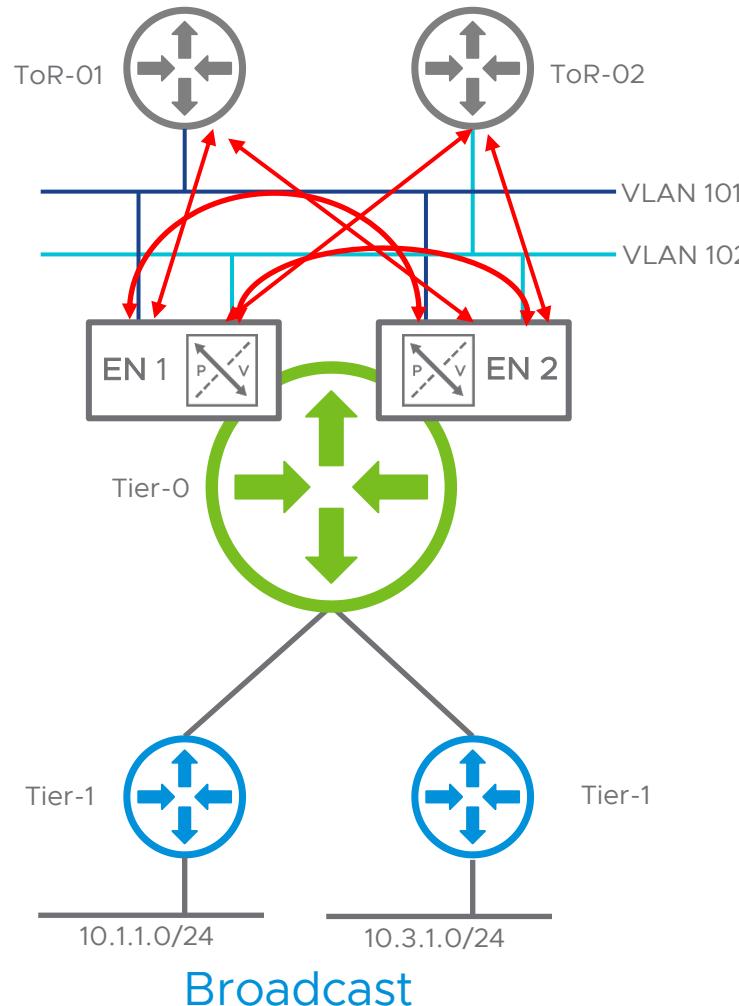
A router will only form an OSPF adjacency on a broadcast network with a DR/BDR

OSPF Adjacencies – Broadcast



```
SRV-EDGE-01(tier0_sr)> get ospf interface  
uplink-288 is up  
    ifindex 24, MTU 9000 bytes, BW 0 Mbit <UP,BROADCAST,RUNNING,MULTICAST>  
    Internet Address 172.16.11.1/24, Broadcast 172.16.11.255, Area 0.0.0.0  
    MTU mismatch detection: enabled  
    Router ID 172.16.11.1, Network Type BROADCAST, Cost: 10  
    Transmit Delay is 1 sec, State DROther, Priority 0  
    Designated Router (ID) 11.11.11.11, Interface Address 172.16.11.11  
    No backup designated router on this network  
    Multicast group memberships: OSPFAllRouters  
    Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5  
        Hello due in 1.007s  
    Neighbor Count is 2, Adjacent neighbor count is 1  
    Authentication NULL is enabled  
uplink-323 is up  
    ifindex 20, MTU 9000 bytes, BW 0 Mbit <UP,BROADCAST,RUNNING,MULTICAST>  
    Internet Address 172.16.10.1/24, Broadcast 172.16.10.255, Area 0.0.0.0  
    MTU mismatch detection: enabled  
    Router ID 172.16.11.1, Network Type BROADCAST, Cost: 10  
    Transmit Delay is 1 sec, State DROther, Priority 0  
    Designated Router (ID) 10.10.10.10, Interface Address 172.16.10.10  
    No backup designated router on this network  
    Multicast group memberships: OSPFAllRouters  
    Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5  
        Hello due in 1.007s  
    Neighbor Count is 2, Adjacent neighbor count is 1  
    Authentication NULL is enabled
```

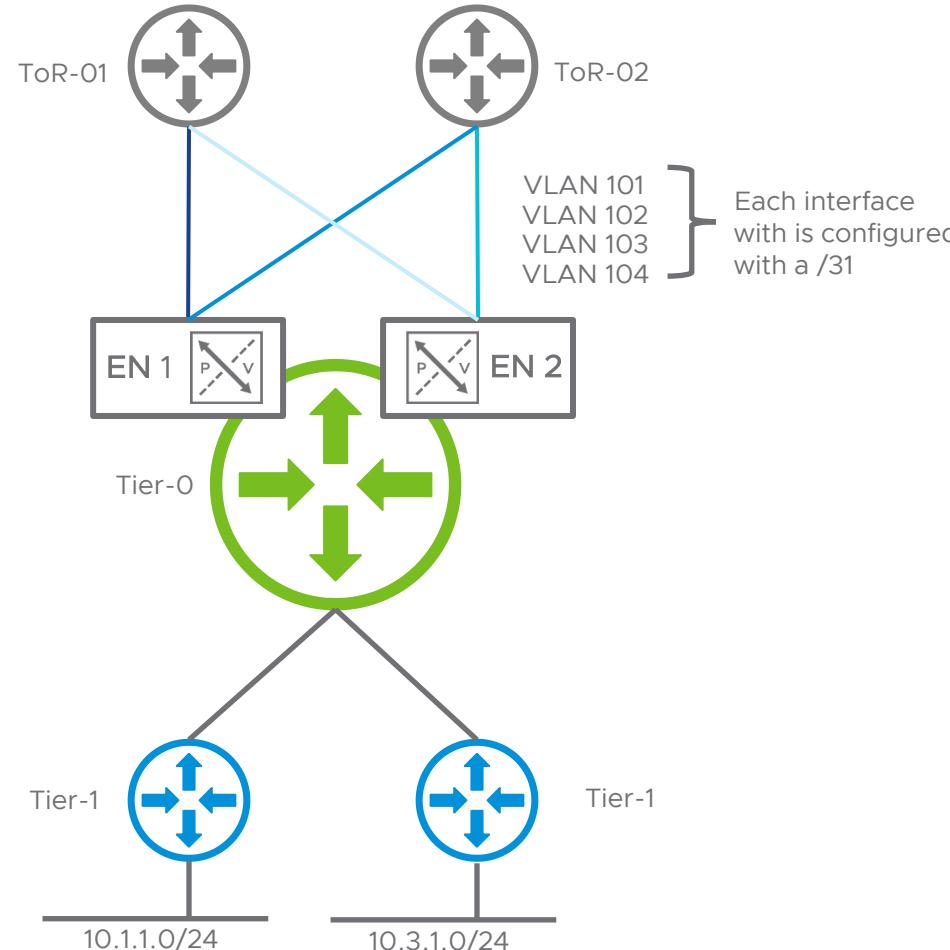
OSPF Adjacencies – Broadcast



SRV-EDGE-01(tier0_sr)> get ospf neigh									
Neighbor ID	Pri	State	UpTime	Dead Time	Address	Interface	RXmtL	RqstL	DBsmL
2.2.2.2	0	2-Way/DROther	4h03m26s	36.806s	172.16.11.2	uplink-288:172.16.11.1	0	0	0
11.11.11.11	1	Full/DR	4h04m07s	31.441s	172.16.11.11	uplink-288:172.16.11.1	0	0	0
2.2.2.2	0	2-Way/DROther	4h03m26s	36.808s	172.16.10.2	uplink-323:172.16.10.1	0	0	0
10.10.10.10	1	Full/DR	4h04m07s	37.409s	172.16.10.10	uplink-323:172.16.10.1	0	0	0

OSPF Adjacencies – Point to Point

NSX-T 3.1.1 support interfaces to be configured as Point to Point. (strongly recommended)



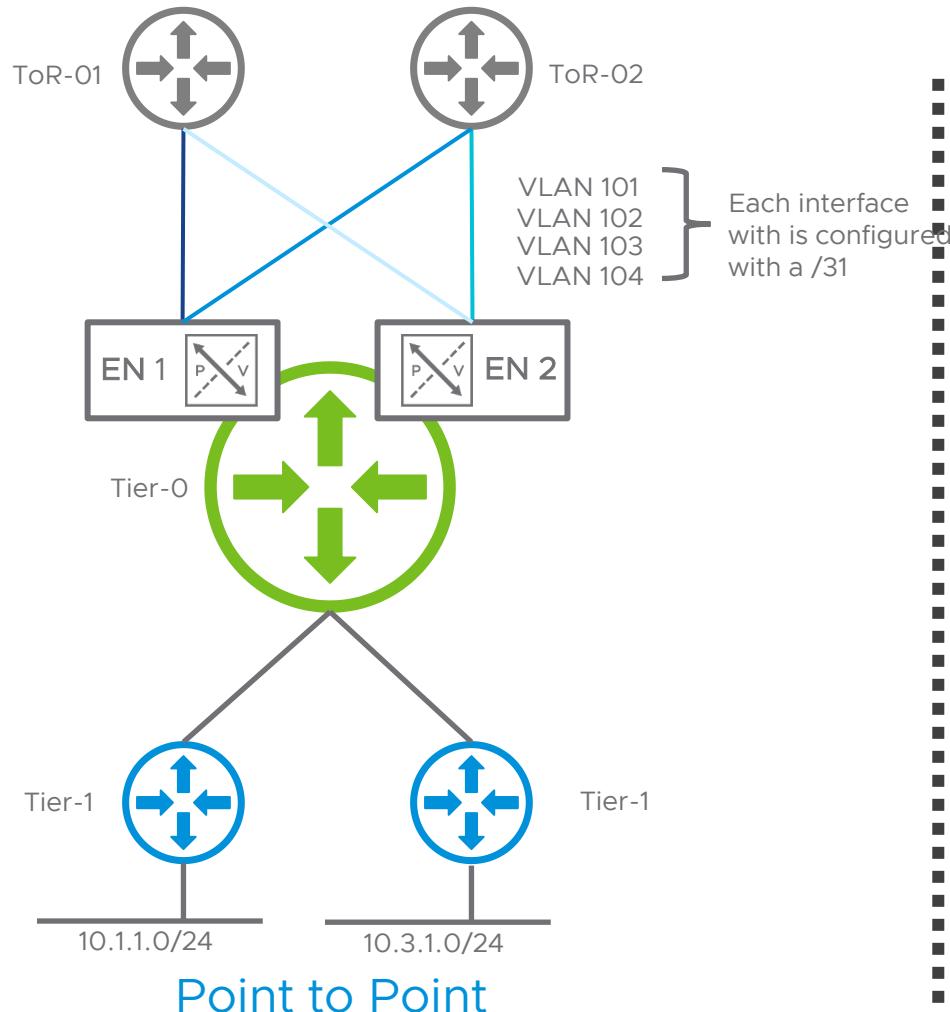
Point to Point

No DR/BDR Election

OSPF Neighbors					
Tier-0 Gateway	Tier0-Tenant...	#Neighbors			
Last Updated On: Feb 2, 2021, 8:47:00 AM					
Neighbor IP Address	Interface	Source	Edge Node	Priority	State
> 10.10.10.10	uplink-401:172.16.11.0	172.16.11.1	EDGE-02	1	Full
> 11.11.11.11	uplink-417:172.16.12.0	172.16.12.1	EDGE-02	1	Full
> 10.10.10.10	uplink-429:172.16.10.0	172.16.10.1	EDGE-01	1	Full
> 11.11.11.11	uplink-427:172.16.13.0	172.16.13.1	EDGE-01	1	Full

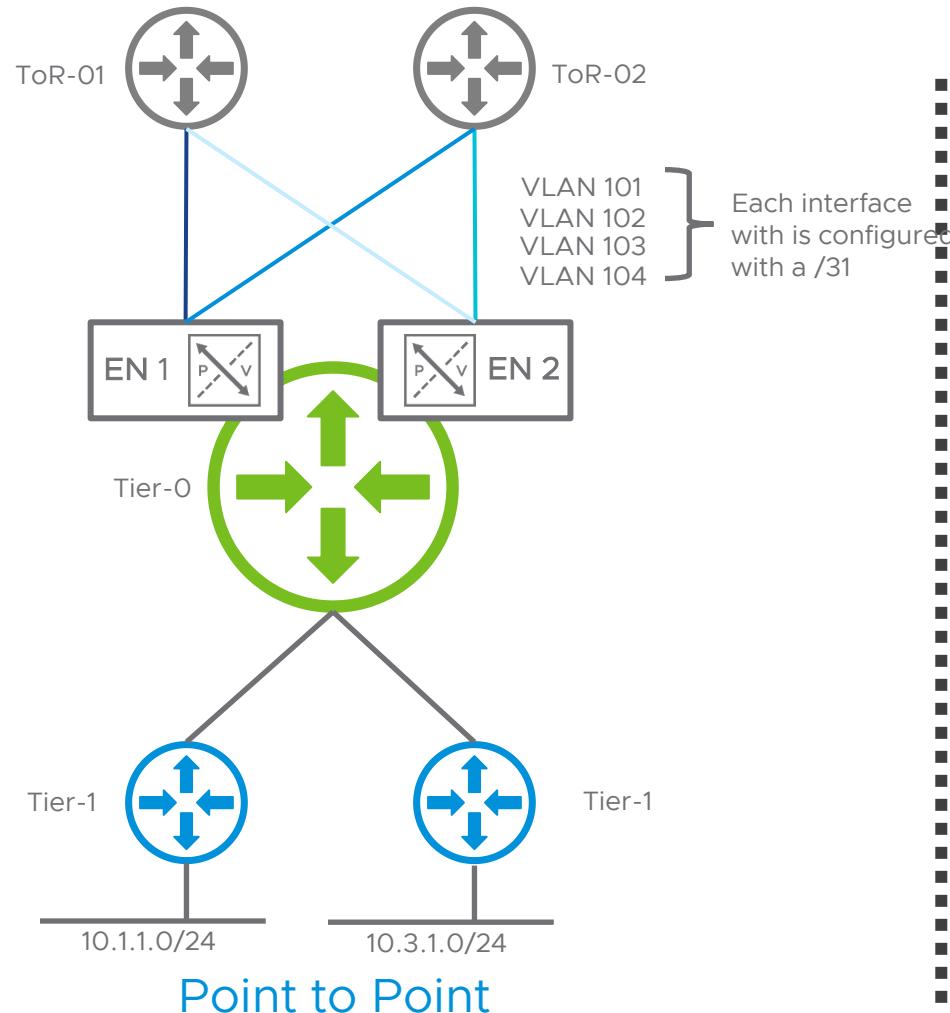
Simpler output and less adjacencies to track

OSPF Adjacencies – Point to Point



```
SRV-EDGE-01(tier0_sr)> get ospf interface  
uplink-427 is up  
  ifindex 37, MTU 9000 bytes, BW 0 Mbit <UP,BROADCAST,RUNNING,MULTICAST>  
  Internet Address 172.16.13.0/31, Area 0.0.0.0  
  MTU mismatch detection: enabled  
  Router ID 1.1.1.1, Network Type POINTTOPPOINT, Cost: 65534  
  Transmit Delay is 1 sec, State Point-To-Point, Priority 0  
  No backup designated router on this network  
  Multicast group memberships: OSPFALLRouters  
  Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5  
    Hello due in 8.667s  
  Neighbor Count is 1, Adjacent neighbor count is 1  
  Authentication NULL is enabled  
uplink-429 is up  
  ifindex 40, MTU 9000 bytes, BW 0 Mbit <UP,BROADCAST,RUNNING,MULTICAST>  
  Internet Address 172.16.10.0/31, Area 0.0.0.0  
  MTU mismatch detection: enabled  
  Router ID 1.1.1.1, Network Type POINTTOPPOINT, Cost: 65534  
  Transmit Delay is 1 sec, State Point-To-Point, Priority 0  
  No backup designated router on this network  
  Multicast group memberships: OSPFALLRouters  
  Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5  
    Hello due in 8.668s  
  Neighbor Count is 1, Adjacent neighbor count is 1  
  Authentication NULL is enabled
```

OSPF Adjacencies – Point to Point



```
SRV-EDGE-01(tier0_sr)> get ospf neighbor
```

Neighbor ID	Pri	State	UpTime	Dead Time	Address	Interface
11.11.11.11	1	Full/-	9m22s	37.788s	172.16.13.1	uplink-427:172.16.13.0
10.10.10.10	1	Full/-	9m30s	39.795s	172.16.10.1	uplink-429:172.16.10.0

OSPF Support in NSX-T 3.1.1

Active-Active and **Active-Standby** topologies are supported.

OSPF v2 only support. IPv6 workloads need BGP and IPv6 address family.

BFD Support with OSPFv2 (BM: 50ms – VM: 500ms – Multiplier: 3)

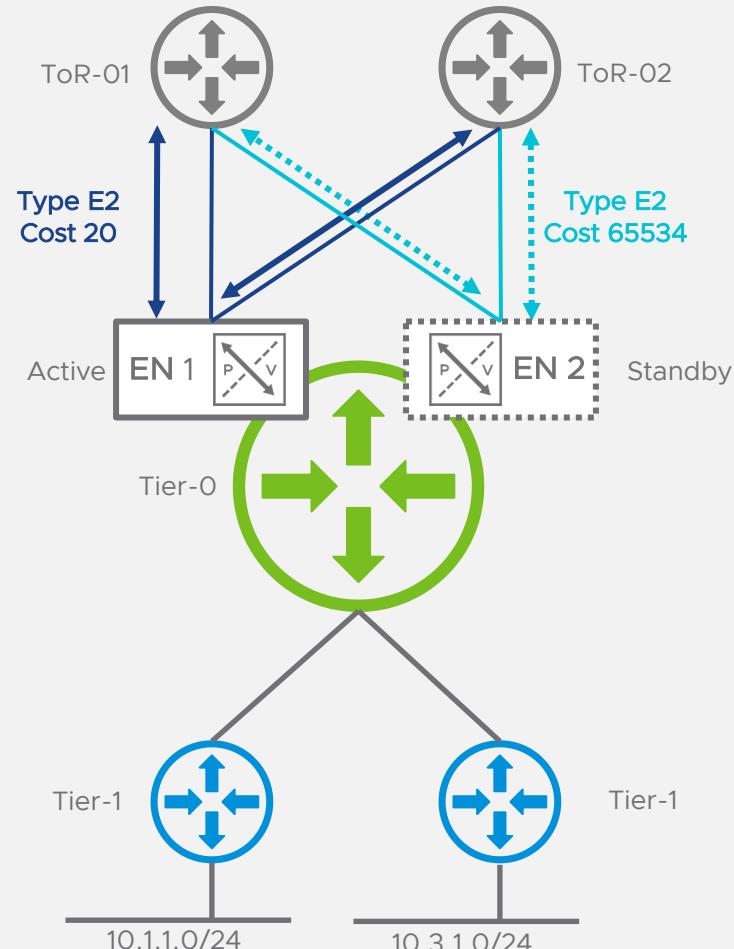
OSPF v2 support in the Parent Tier-0 Gateway only.

- Not currently supported on a Tier-0 VRF.
- Not currently supported for Federation.

A **Single Area per Tier-0** is supported (No ABR functionality). No Inter SR Routing needed (LSDB is identical within an area).

- Backbone (Area 0)
- Non-Backbone
- NSSA (Not so Stubby)

Active/Standby Topology

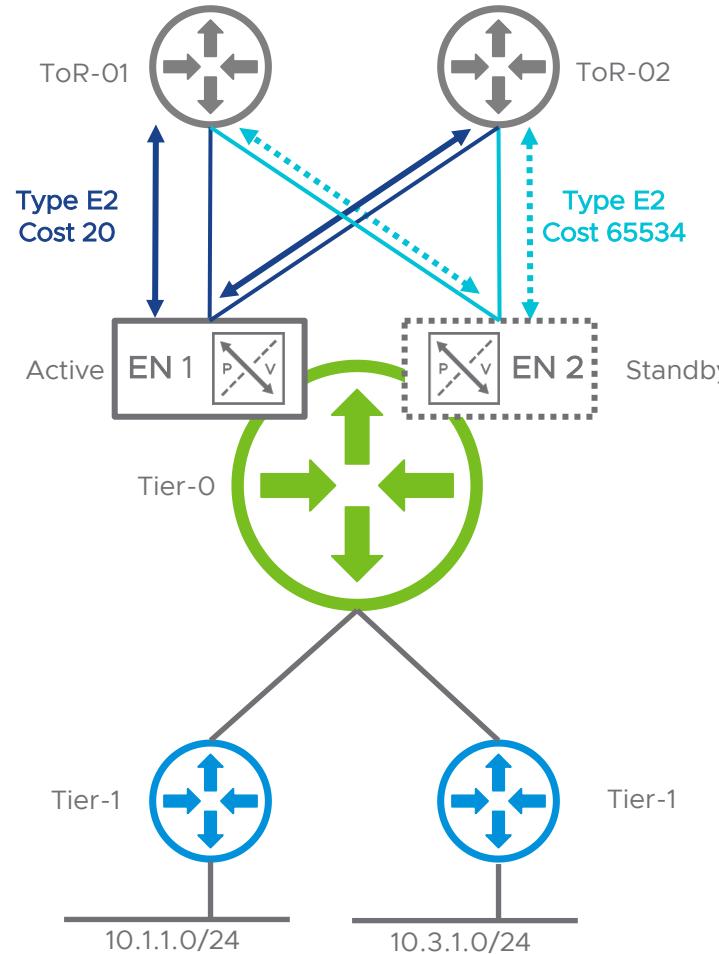


Standby Tier-0 is still active from an OSPF standpoint.

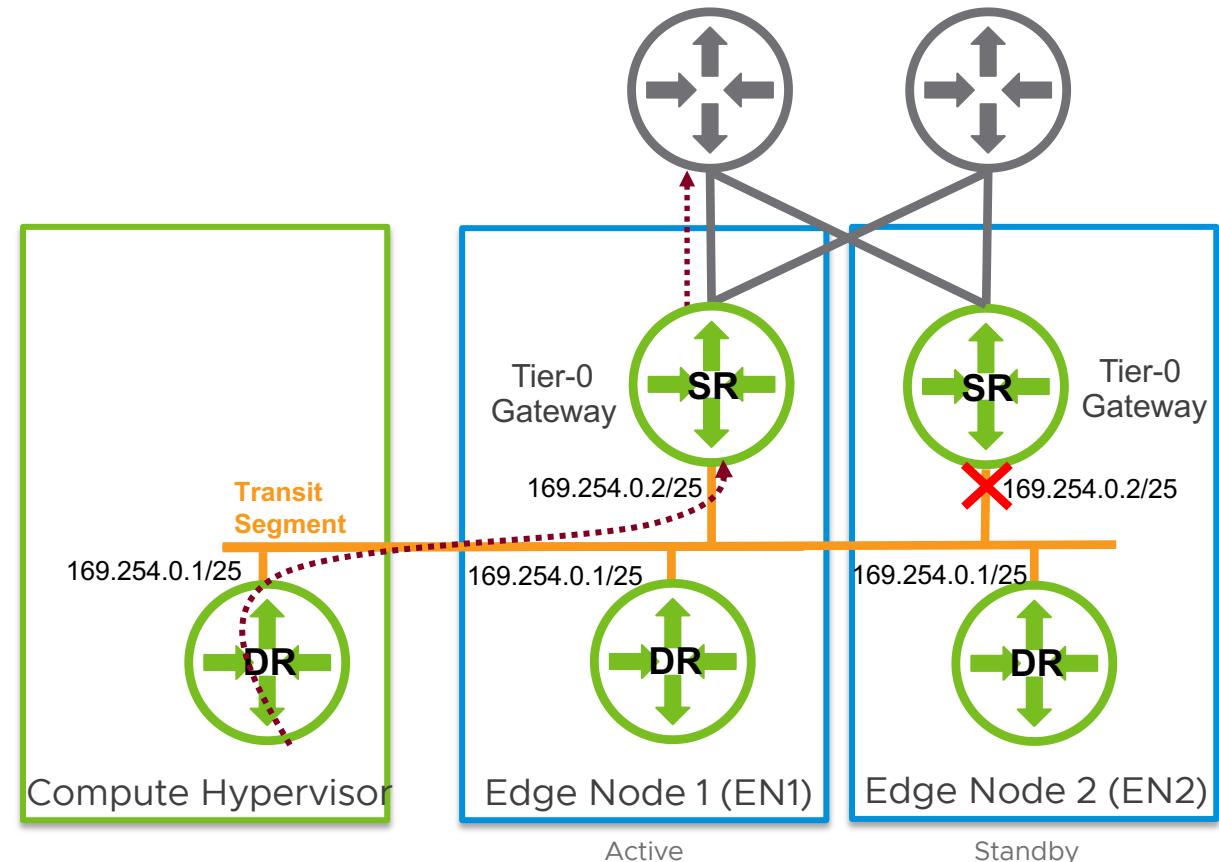
Standby Tier-0 will use OSPF cost to influence routing decision on ToR-A and ToR-B.

Metrics sent by standby Tier-0 is 65534

Logical Topology



Physical Topology



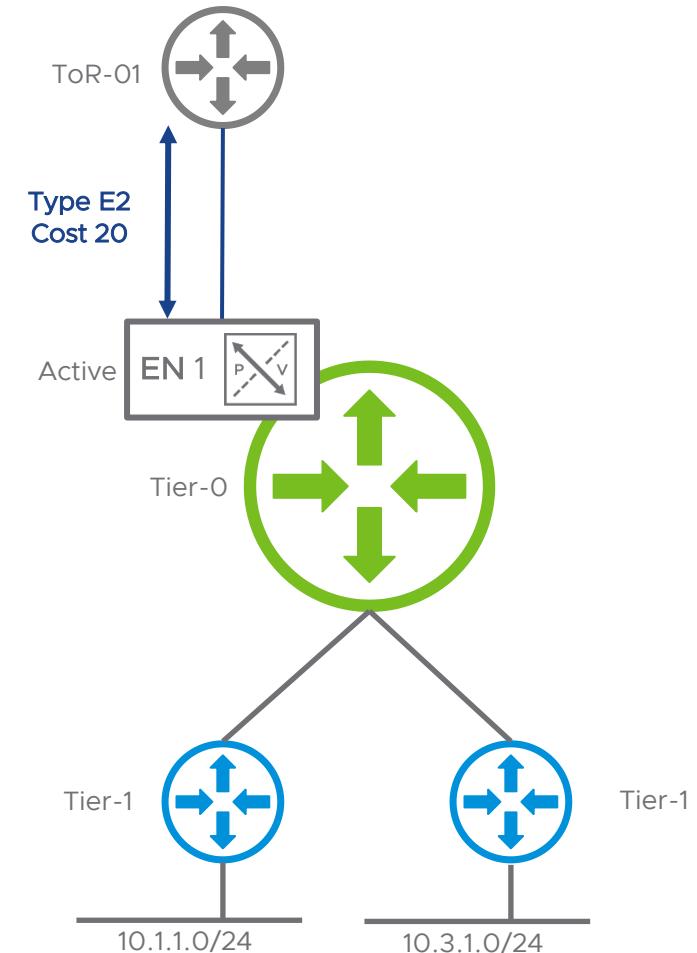
Active/Standby Topology – ToR Verification

```
cumulus@TOR-01:mgmt:~$ net show ospf database external 10.1.1.0

      AS External Link States

  LS age: 164
  Options: 0x2 : *|-|-|-|-|E|-|
  LS Flags: 0x6
LS Type: AS-external-LSA
  Link State ID: 10.1.1.0 (External Network Number)
  Advertising Router: 172.16.11.1
  LS Seq Number: 80000005
  Checksum: 0x9095
  Length: 36

  Network Mask: /24
    Metric Type: 2 (Larger than any link state path)
    TOS: 0
Metric: 20
    Forward Address: 0.0.0.0
    External Route Tag: 4016
```



Active/Standby Topology – Edge Verification CLI

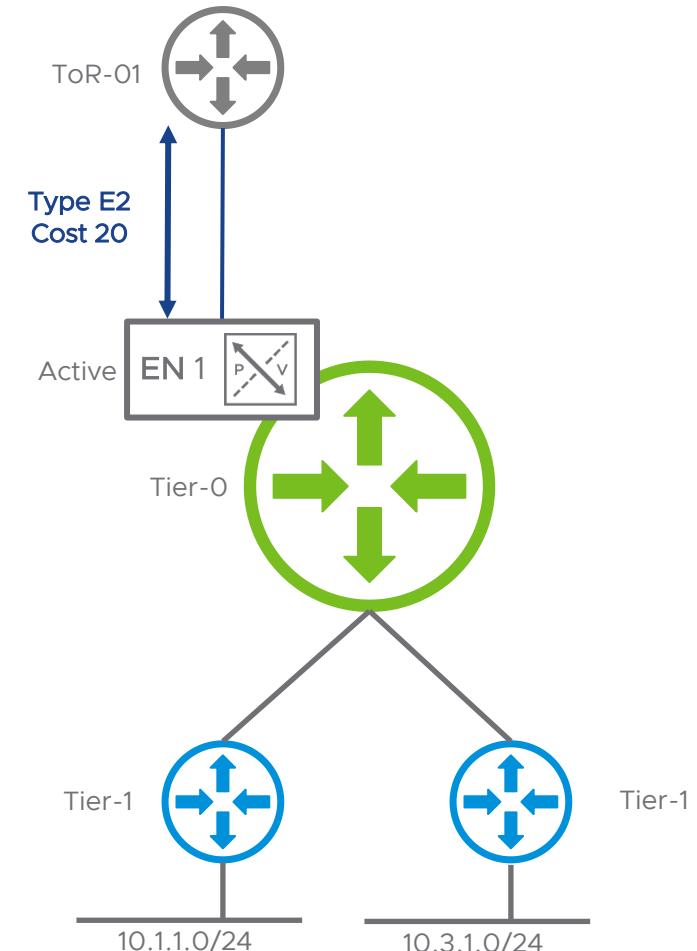
```
SRV-EDGE-01(tier0_sr)> get ospf database external 10.1.1.0
```

OSPF Router with ID (172.16.11.1)

AS External Link States

```
LS age: 296
Options: 0x2 : *|-|-|-|-|E|-
LS Flags: 0xb
LS Type: AS-external-LSA
Link State ID: 10.1.1.0 (External Network Number)
Advertising Router: 172.16.11.1
LS Seq Number: 80000013
Checksum: 0x74a3
Length: 36
```

```
Network Mask: /24
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 20
Forward Address: 0.0.0.0
External Route Tag: 4016
```



Active/Standby Topology – ToR Verification

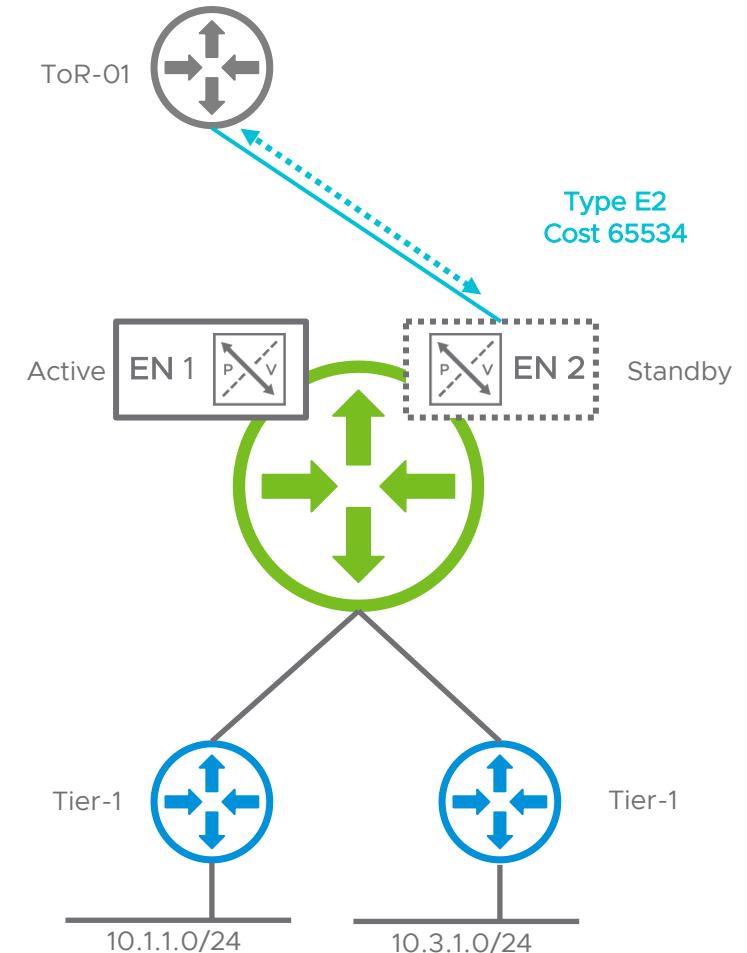
```
cumulus@TOR-01:mgmt:~$ net show ospf database external 10.1.1.0
```

AS External Link States

```
LS age: 129
Options: 0x2 : *|-|-|-|-|E|-|
LS Flags: 0x6
LS Type: AS-external-LSA
Link State ID: 10.1.1.0 (External Network Number)
Advertising Router: 2.2.2.2
LS Seq Number: 80000007
Checksum: 0x6396
Length: 36
```

Network Mask: /24

```
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 65534
Forward Address: 0.0.0.0
External Route Tag: 4016
```



Active/Standby Topology – ToR Verification

```
SRV-EDGE-02(tier0_sr)> get ospf database external 10.1.1.0
```

OSPF Router with ID (2.2.2.2)

AS External Link States

```
LS age: 992
Options: 0x2 : *|-|-|-|-|E|
LS Flags: 0xb
LS Type: AS-external-LSA
Link State ID: 10.1.1.0 (External Network Number)
Advertising Router: 2.2.2.2
LS Seq Number: 80000018
Checksum: 0x41a7
Length: 36
```

Network Mask: /24

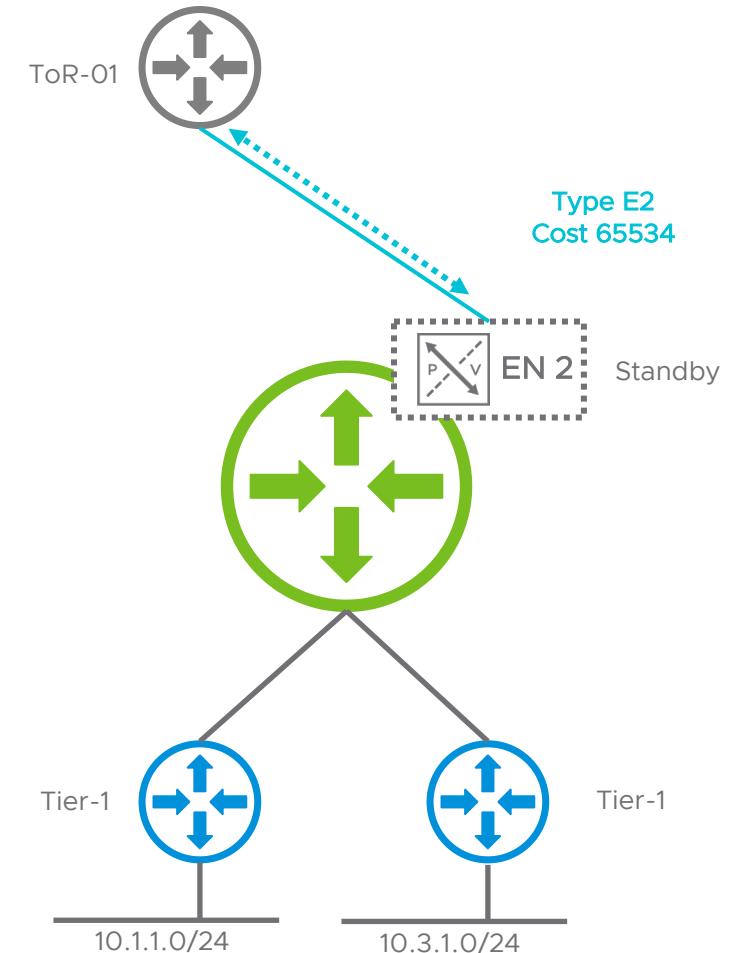
Metric Type: 2 (Larger than any link state path)

TOS: 0

Metric: 65534

Forward Address: 0.0.0.0

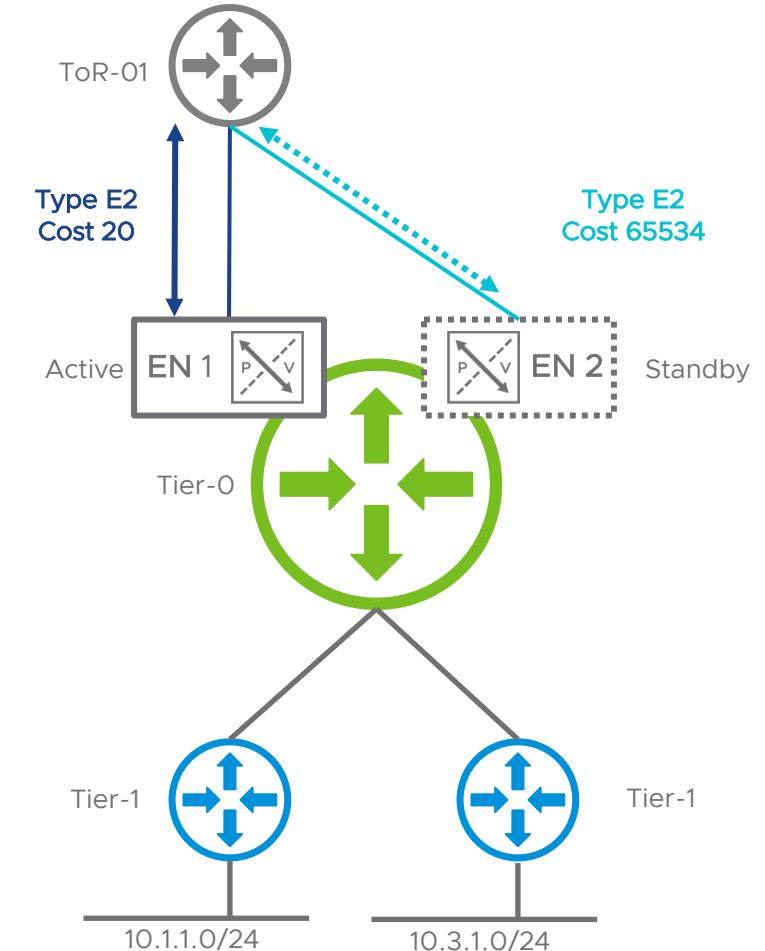
External Route Tag: 4016



Active/Standby Topology – ToR Verification

```
cumulus@TOR-01:mgmt:~$ net show route 10.1.1.0
RIB entry for 10.1.1.0
=====
Routing entry for 10.1.1.0/24
  Known via "ospf", distance 110, metric 20, tag 4016, best
  Last update 00:46:12 ago
* 172.16.10.1, via swp1.10, weight 1

FIB entry for 10.1.1.0
=====
10.1.1.0/24 via 172.16.10.1 dev swp1.10 proto ospf metric 20
```



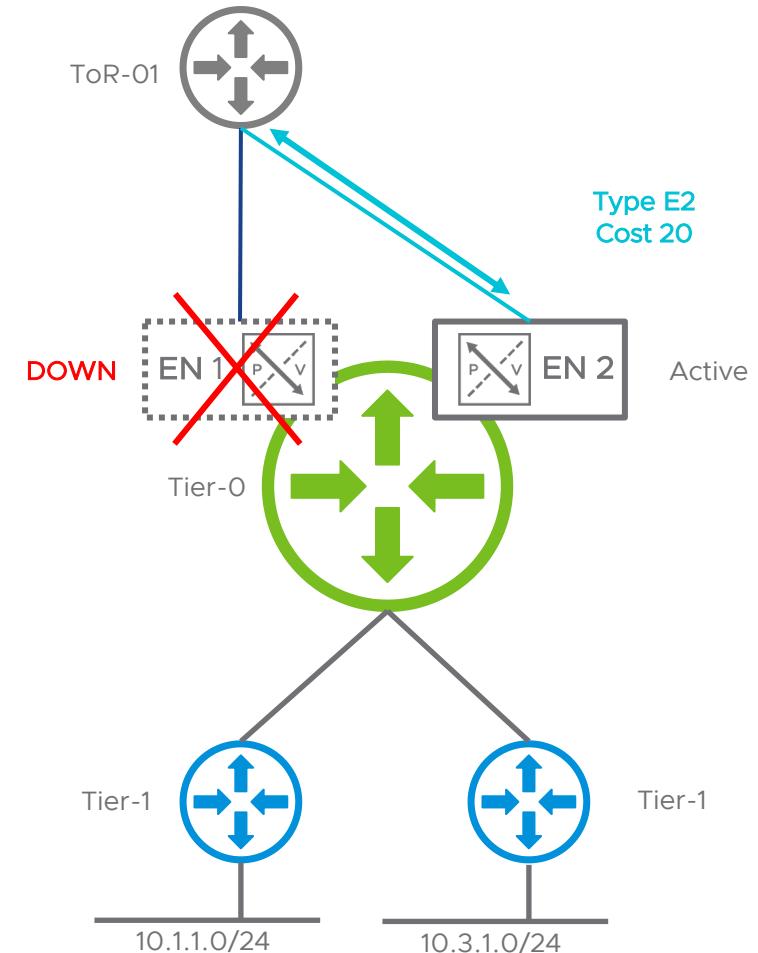
Active/Standby Topology – ToR Verification

```
cumulus@TOR-01:mgmt:~$ net show ospf database external 10.1.1.0
OSPF Router with ID (10.10.10.10)

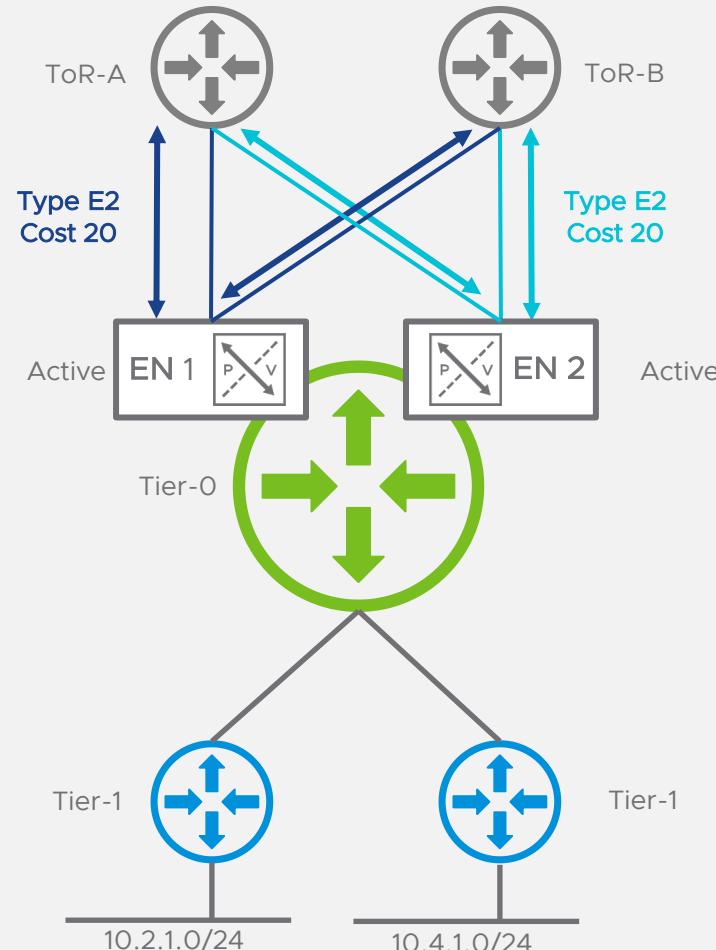
AS External Link States

LS age: 10
Options: 0x2 : *|-|-|-|-|E|-
LS Flags: 0x6
LS Type: AS-external-LSA
Link State ID: 10.1.1.0 (External Network Number)
Advertising Router: 2.2.2.2
LS Seq Number: 8000000c
Checksum: 0x2cb3
Length: 36

Network Mask: /24
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 20
Forward Address: 0.0.0.0
External Route Tag: 4016
```



Active/Active Topology

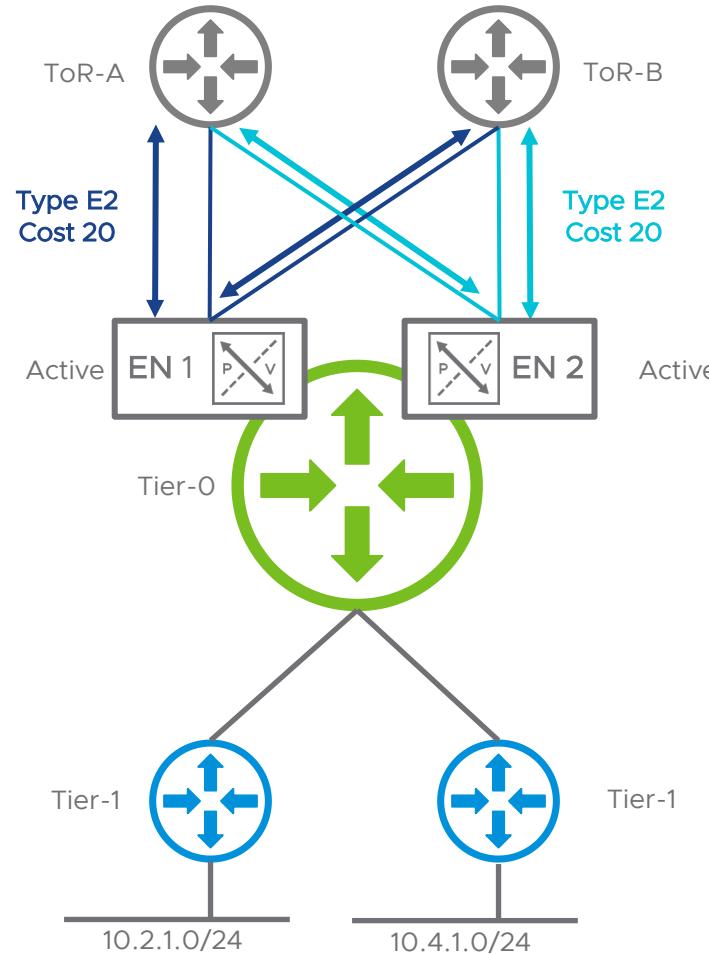


OSPF ECMP supports 8 links
(2 interfaces can be enabled for OSPF per edge node)

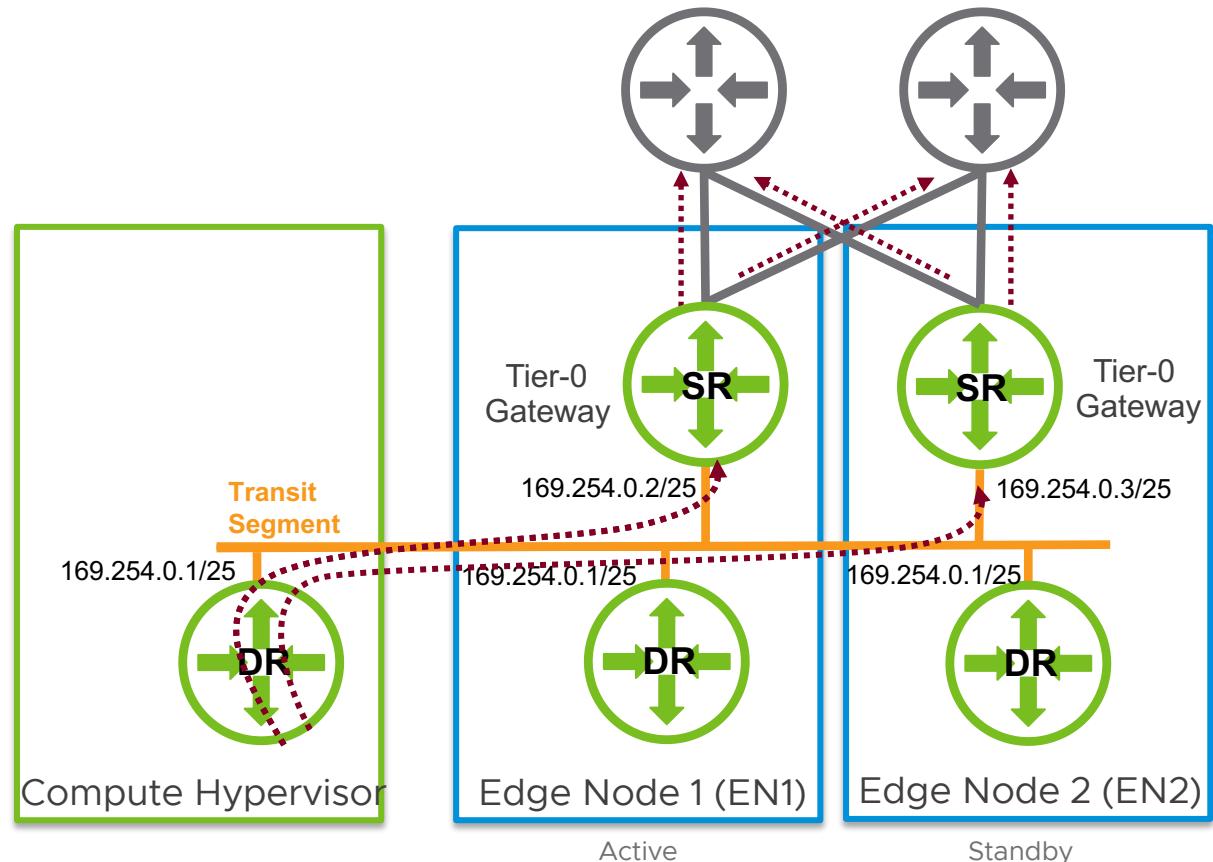
Metric sent by all the Tier-0 LR is 20

Active/Active Topology

Logical Topology



Physical Topology



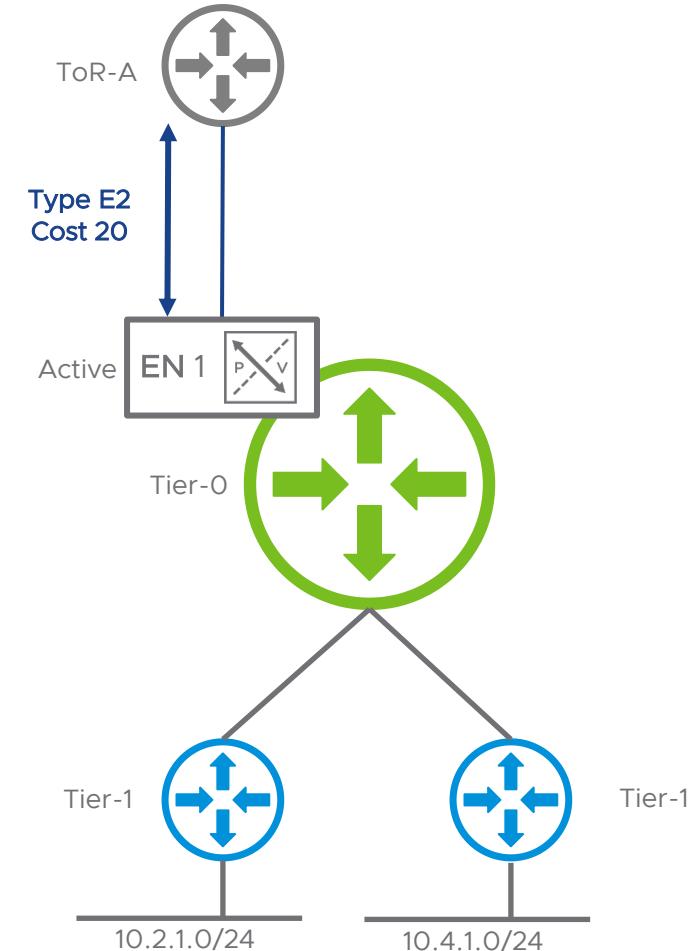
Active/Active Topology – ToR Verification

```
cumulus@TOR-03:mgmt:~$ net show ospf database external 10.2.1.0
OSPF Router with ID (20.20.20.20)

AS External Link States

LS age: 449
Options: 0x2 : *|-|-|-|-|E|-
LS Flags: 0x6
LS Type: AS-external-LSA
Link State ID: 10.2.1.0 (External Network Number)
Advertising Router: 172.16.20.3
LS Seq Number: 80000001
Checksum: 0x41dc
Length: 36

Network Mask: /24
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 20
Forward Address: 0.0.0.0
External Route Tag: 4016
```



Active/Active Topology – ToR Verification

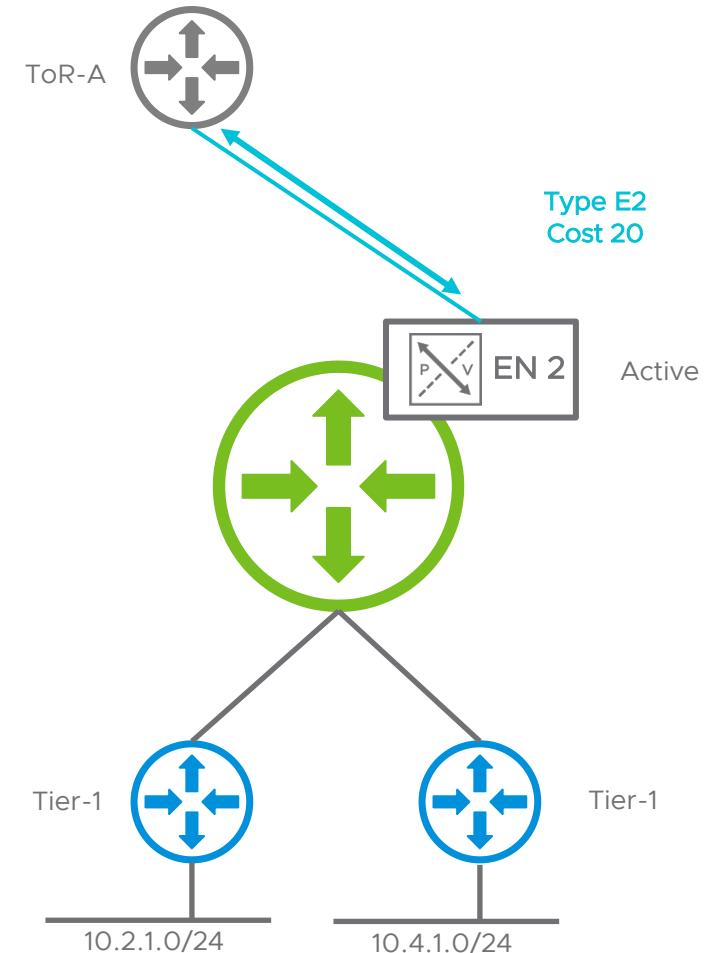
```
cumulus@TOR-01:mgmt:~$ net show ospf database external 10.1.1.0
```

AS External Link States

```
LS age: 448
Options: 0x2 : *|-|-|-|-|E|-|
LS Flags: 0x6
LS Type: AS-external-LSA
Link State ID: 10.2.1.0 (External Network Number)
Advertising Router: 172.16.21.4
LS Seq Number: 80000001
Checksum: 0x34e7
Length: 36
```

Network Mask: /24

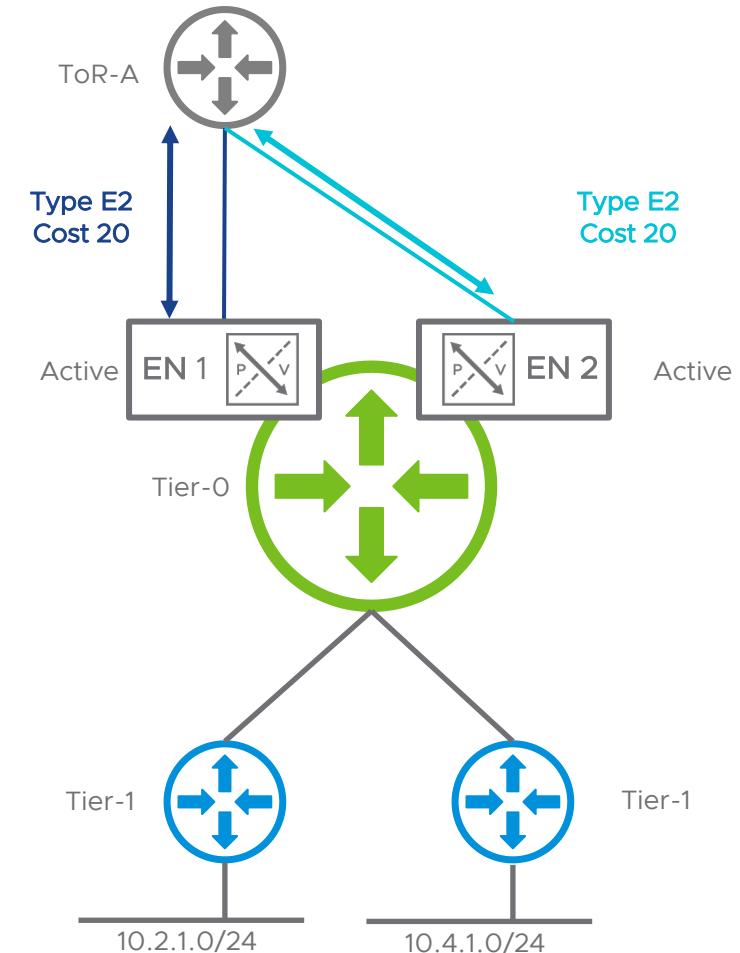
```
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 20
Forward Address: 0.0.0.0
External Route Tag: 4016
```



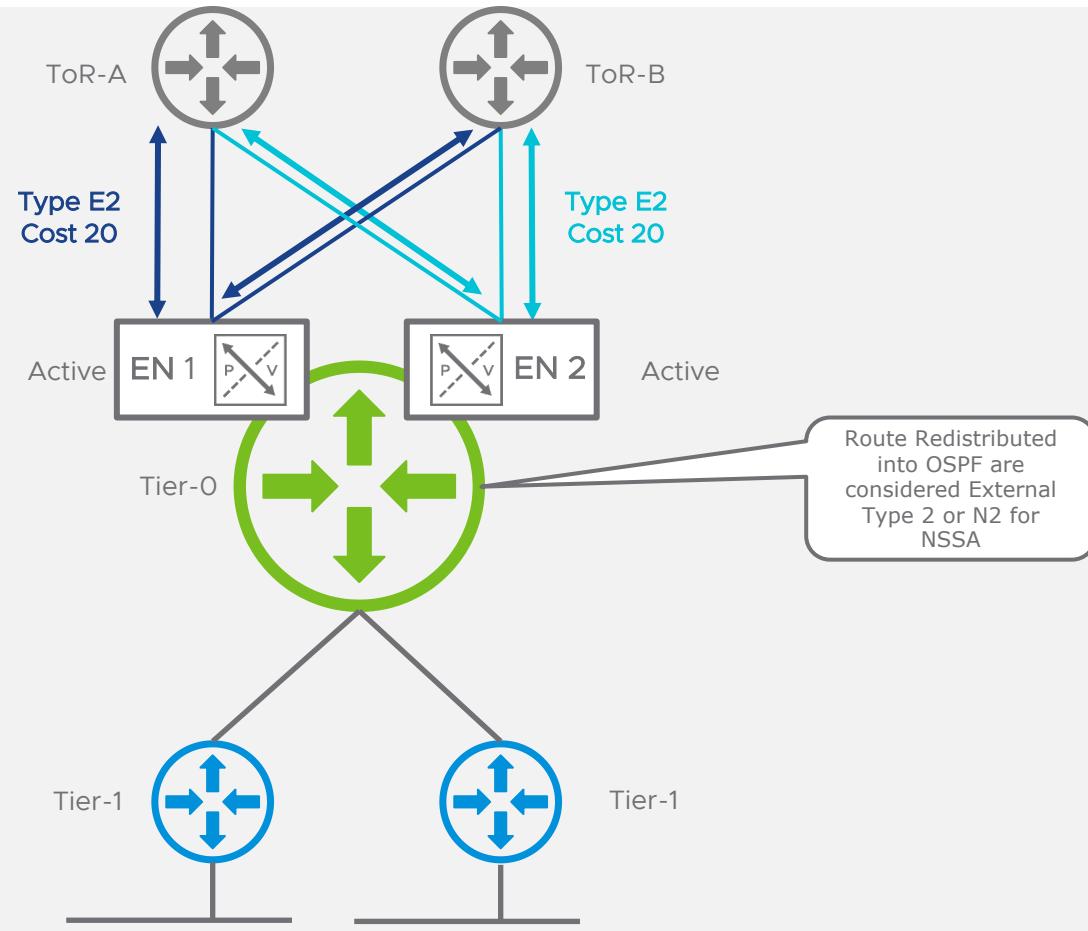
Active/Active Topology – ToR Verification

```
cumulus@TOR-03:~$ net show route 10.2.1.0
RIB entry for 10.2.1.0
=====
Routing entry for 10.2.1.0/24
  Known via "ospf", distance 110, metric 20, tag 4016, best
  Last update 00:32:15 ago
  * 172.16.20.3, via swp1.20, weight 1
  * 172.16.20.4, via swp1.20, weight 1

FIB entry for 10.2.1.0
=====
10.2.1.0/24 proto ospf metric 20
  nexthop via 172.16.20.3 dev swp1.20 weight 1
  nexthop via 172.16.20.4 dev swp1.20 weight 1
```



Route Redistribution



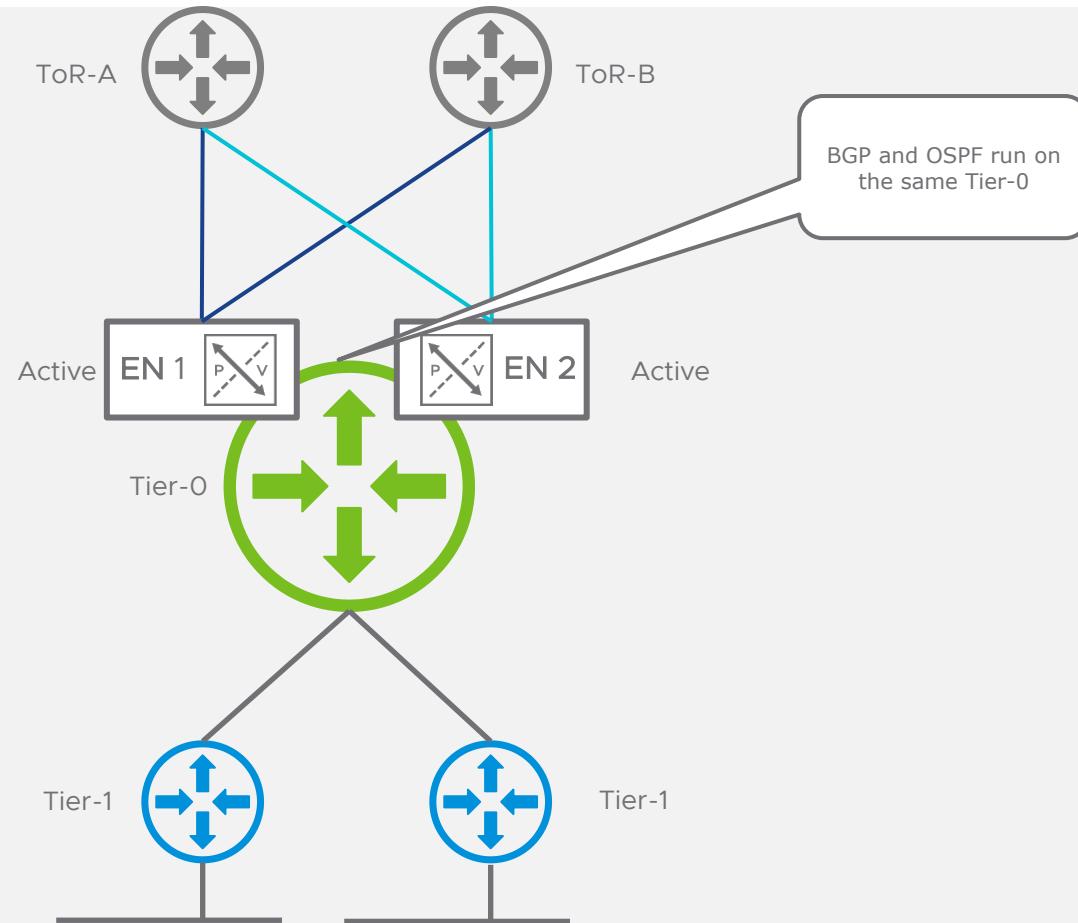
Tier-1 Segments are considered static routes from a Tier-0 standpoint.

These static routes are redistributed into OSPF on the Tier-0. **The routes type is E2 or N2 for NSSA areas.**

E2 and N2:

- Cost is always 20 (vs E1 where the internal links cost would be added on each router)

Route Redistribution

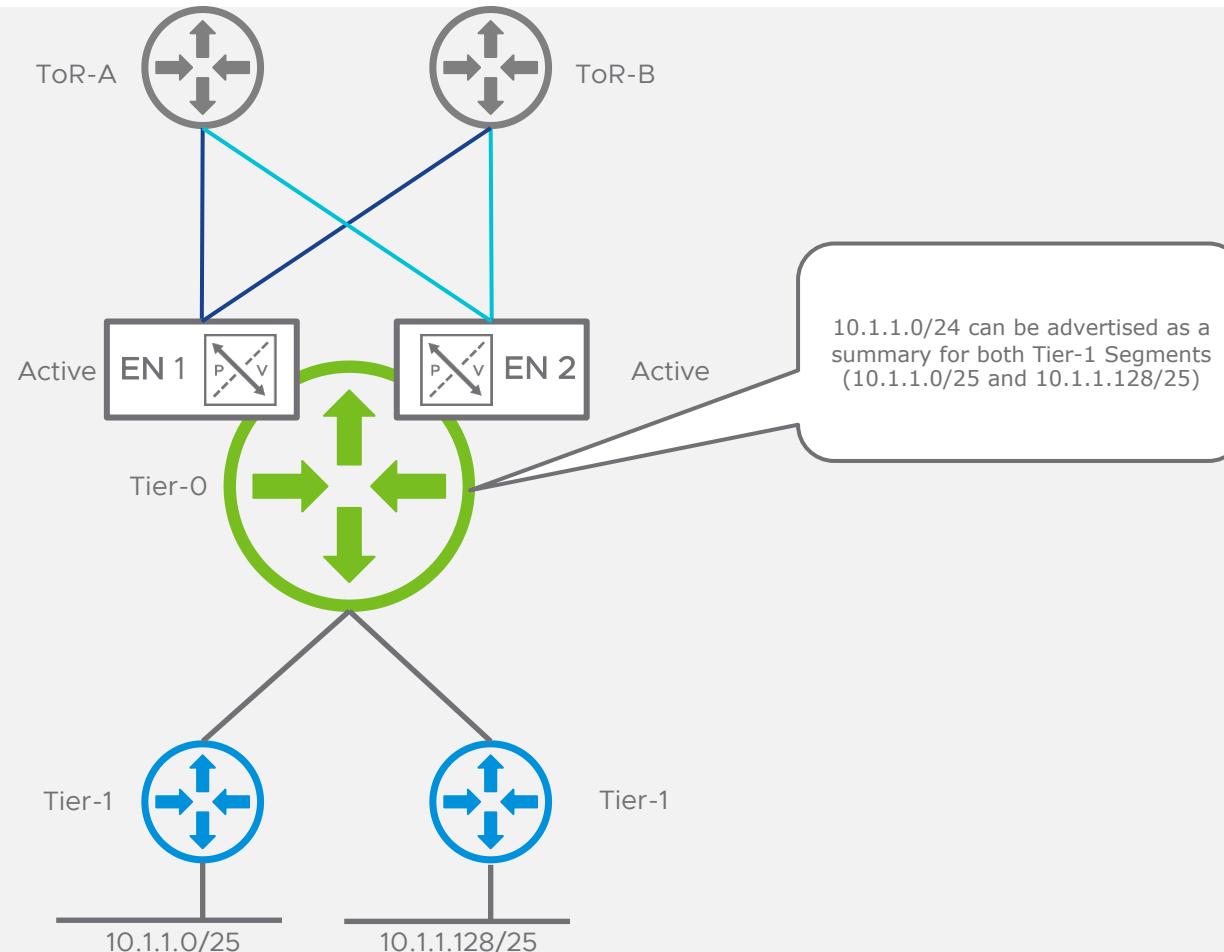


Redistribution between BGP and OSPF is not supported.

It is possible to use OSPF to learn the BGP Peer IP address in case of BGP multi-hop design.

Running both protocols can complicate operations (Hint: Administrative Distance).

Route Summarization



Summarization is supported on the Tier-0.

LSA for that summary route will still be advertised as a type 5 LSA in a standard area.

Configuration – BFD Profile

NSX-T

Networking Profiles

BFD Profile

Name	Interval	Declare Dead Multiple	Status
default	500	3	Uninitialized
OSPF	500	3	*

Description: Enter Description

Tags: Max 30 allowed. Click (+) to add.

SAVE CANCEL

Possible to use either the Default or custom BFD Profile.

BFD Support with OSPFv2
(BM: 50ms – VM: 500ms – Multiplier: 3)

Configuration – Redistribution

The screenshot shows the 'Tier-0 Gateways' configuration page. The 'Tier-0 Tenant' dropdown is set to 'Tier0-Tenant01' and 'Active Status' is selected. Under 'Fail Over' settings, 'Preemptive' is chosen. The 'HA Mode' is set to 'Edge-Cluster-01'. 'DHCP' is enabled with 'Set DHCP Configuration'. 'Preferred Edge' is set to 'Select Edge Node'. In the 'Description' field, it says 'Tier0 provisioned by Terraform'. The 'ROUTE RE-DISTRIBUTION' section is expanded, showing 'BGP' and 'OSPF' both enabled. A 'Route Re-distribution' status bar indicates 1 route redistributed. An 'OSPF Route Redistribution Status' button is turned 'On'. A note at the bottom says 'Changes Saved!'. On the left sidebar, 'ROUTING' is expanded, showing 'BGP' and 'OSPF' status.

Set Route Re-distribution

Name	Destination Protocol	Route Re-distribution	Route Map
TO-Default-Redistribution	BGP X OSPF X	9*	Select Route Map

ADD CANCEL

T1 segments needs to be redistributed in the OSPF process (same as BGP).

Prefixes will be advertised as **E2 or N2** into OSPF

Configuration – Area Definition

The screenshot shows the 'Tier-0 Gateways' configuration page. The 'Tier-0 Tenant01' gateway is selected. In the 'OSPF' section, the 'Enabled' radio button is selected. A 'Set' button is visible next to the 'Area Definition' label, which is highlighted with a blue dashed box.

Area Definition:

- 1 Area per Tier-0 Gateway
 - Standard
 - Backbone (0)
 - NSSA

Configuration – Area Definition

The screenshot shows the 'Set Area Definition' dialog box. At the top, there are navigation links: 'Tier-0 Gateway', 'Tier0-Tenant...', and '#Area Definitions 1'. Below the title 'Set Area Definition' is a search bar with a magnifying glass icon and the word 'Search'. The main form has the following fields:

Area ID	Type	Authentication	Key ID	Password	Status
0	* Normal	MD5	1	(Info icon)

Below the table, there are 'Description' and 'Tags' sections. The 'Tags' section contains a 'Tag' button, a 'Scope' dropdown, and a note: 'Max 30 allowed. Click (+) to add.' At the bottom of the dialog are 'SAVE' and 'CANCEL' buttons.

Area Definition:

- Area ID: Single Number (0) or dotted format (0.0.0.0)

Type:

- Normal or NSSA

Authentication:

- MD5 (hashing) or Password (plain text)

Key ID

Password: 8 Characters Max in MD5 and Password (PM/TPM discussing with Engineering to increase the number of characters)

Configuration – Interfaces

The screenshot shows the 'Set OSPF Configured Interfaces' interface. It lists four interfaces under the 'Tier-0 Tenant...' tab:

Interface	Area ID	Network Type	OSPF Status	BFD Profile	OSPF Dead Interval (Seconds)	Status
EN02-TOR01-VLAN11	0	P2P	Enabled	OSPF	40	Success
EN02-TOR02-VLAN12	0	P2P	Enabled	OSPF	40	Success
EN01-TOR01-VLAN10	0	P2P	Enabled	OSPF	40	Success
EN01-TOR02-VLAN13	0	P2P	Enabled	OSPF	40	Success

Annotations highlight two groups of interfaces:

- EN02 - Interfaces**: Points to the first two rows (EN02-TOR01-VLAN11 and EN02-TOR02-VLAN12).
- EN01 - Interfaces**: Points to the last two rows (EN01-TOR01-VLAN10 and EN01-TOR02-VLAN13).

2 OSPF Interfaces per Edge Nodes maximum

Area:

- Same Area on all uplinks for a dedicated Tier-0

Network Type:

- P2P strongly recommended. Not recommended to mix network type

BFD: Profile must be used

The screenshot shows the 'Tier-0 Gateways' configuration page. The gateway 'Tier0-Tenant01' is listed with the following details:

Tier-0 Gateway Name	HA Mode	Linked Tier-1 Gateways	Linked Segments	Status	Alarms
Tier0-Tenant01	Active Standby	2	0	Success	0

Under the 'ROUTING' section, OSPF is explicitly enabled:

Protocol	Status
BGP	Enabled
OSPF	Enabled

Other configuration options shown include:

- Fail Over: Preemptive
- Edge Cluster: Edge-Cluster-01
- HA VIP Configuration: 0
- Additional Settings, Route Distinguisher for VRF Gateways, EVPN Settings
- Description: Tier0 provisioned by Terraform
- Tags: 0
- INTERFACES, ROUTING, BGP, OSPF, ECMP, Default Route Originate, OSPF Neighbors
- ROUTE RE-DISTRIBUTION, MULTICAST

Protocol is not enabled by default when creating a Tier-0. OSPF must be toggled on.

Useful commands

```
SRV-EDGE-01(tier0_sr)> get ospf
OSPF Routing Process, Router ID: 172.16.13.0
Supports only single TOS (TOS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is disabled
OpaqueCapability flag is enabled
Initial SPF scheduling delay 0 millisec(s)
Minimum hold time between consecutive SPFs 50 millisec(s)
Maximum hold time between consecutive SPFs 5000 millisec(s)
Hold time multiplier is currently 2
SPF algorithm last executed 3m53s ago
Last SPF duration 0.002s
SPF timer is inactive
LSA minimum interval 5000 msec
LSA minimum arrival 1000 msec
Write Multiplier set to 20
Refresh timer 10 secs
Maximum multiple paths(ECMP) supported 8
This router is an ASBR (injecting external routing information)
Number of external LSA 36. Checksum Sum 0x0011b03f
Number of opaque AS LSA 0. Checksum Sum 0x00000000
Number of areas attached to this router: 1
Area ID: 0.0.0.0 (Backbone)
    Number of interfaces in this area: Total: 2, Active: 2
    Number of fully adjacent neighbors in this area: 2
    SPF algorithm executed 53 times
    Number of LSA 13
    Number of router LSA 9. Checksum Sum 0x00047b79
    Number of network LSA 4. Checksum Sum 0x0002c314
    Number of summary LSA 0. Checksum Sum 0x00000000
    Number of ASBR summary LSA 0. Checksum Sum 0x00000000
    Number of NSSA LSA 0. Checksum Sum 0x00000000
    Number of opaque link LSA 0. Checksum Sum 0x00000000
    Number of opaque area LSA 0. Checksum Sum 0x00000000
```

```
SRV-EDGE-01(tier0_sr)> get ospf interface
uplink-611 is up
    ifindex 66, MTU 9000 bytes, BW 0 Mbit <UP,BROADCAST,RUNNING,MULTICAST>
    Internet Address 172.16.13.0/31, Area 0.0.0.0
    MTU mismatch detection: enabled
    Router ID 172.16.13.0, Network Type POINTPOINT, Cost: 10
    Transmit Delay is 1 sec, State Point-To-Point, Priority 0
    No backup designated router on this network
    Multicast group memberships: OSPFAllRouters
    Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5
        Hello due in 9.911s
    Neighbor Count is 1, Adjacent neighbor count is 1
    Cryptographic authentication enabled
        Algorithm:MD5, keyId:1 Keydata:VMOSPF
uplink-634 is up
    ifindex 69, MTU 9000 bytes, BW 0 Mbit <UP,BROADCAST,RUNNING,MULTICAST>
    Internet Address 172.16.10.0/31, Area 0.0.0.0
    MTU mismatch detection: enabled
    Router ID 172.16.13.0, Network Type POINTPOINT, Cost: 10
    Transmit Delay is 1 sec, State Point-To-Point, Priority 0
    No backup designated router on this network
    Multicast group memberships: OSPFAllRouters
    Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5
        Hello due in 9.911s
    Neighbor Count is 1, Adjacent neighbor count is 1
    Cryptographic authentication enabled
        Algorithm:MD5, keyId:1 Keydata:VMOSPF
```

Useful commands

```
SRV-EDGE-01(tier0_sr)> get ospf neighbor
```

Neighbor ID	Pri	State	UpTime	Dead Time	Address	Interface	RXmtL	RqstL	DBsmL
11.11.11.11	1	Full/-	2h19m59s	35.092s	172.16.13.1	uplink-611:172.16.13.0	0	0	0
10.10.10.10	1	Full/-	2h19m58s	34.846s	172.16.10.1	uplink-634:172.16.10.0	0	0	0

Useful commands

```
SRV-EDGE-01(tier0_sr)> get ospf database
```

```
    OSPF Router with ID (172.16.13.0)
```

```
        Router Link States (Area 0.0.0.0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Link count
3.3.3.3	3.3.3.3	674	0x80000018	0xc31e	4
10.10.10.10	10.10.10.10	1029	0x80000013	0x0971	5
11.11.11.11	11.11.11.11	1008	0x80000013	0xacb9	5
20.20.20.20	20.20.20.20	678	0x8000001e	0x2969	5
21.21.21.21	21.21.21.21	677	0x8000001e	0x126c	5
100.100.100.100	100.100.100.100	1529	0x80000017	0x8e4c	5
172.16.12.0	172.16.12.0	320	0x80000020	0xa65e	4
172.16.13.0	172.16.13.0	836	0x8000001b	0xa437	4
172.16.22.0	172.16.22.0	679	0x80000018	0xc390	4

```
        Net Link States (Area 0.0.0.0)
```

Link ID	ADV Router	Age	Seq#	CkSum
172.16.3.10	10.10.10.10	1519	0x80000007	0x8820
172.16.4.11	11.11.11.11	1608	0x80000007	0x8717
172.16.5.20	20.20.20.20	1610	0x80000007	0xd675
172.16.6.21	21.21.21.21	1618	0x80000007	0xd56c

```
        AS External Link States
```

Link ID	ADV Router	Age	Seq#	CkSum	Route
0.0.0.0	100.100.100.100	1569	0x80000007	0x1d1d	E2 0.0.0.0/0 [0x0]
1.1.1.1	172.16.13.0	896	0x8000000b	0x7b6b	E2 1.1.1.1/32 [0x0]
2.2.2.2	172.16.12.0	310	0x8000000e	0x7b7a	E2 2.2.2.2/32 [0x0]

Useful commands

```
SRV-EDGE-01(tier0_sr)> get ospf route
Codes: R - Router, N - Network, D - Discard,
       IA - Inter Area, E1 - Type1 external, E2 - Type2 external,
       N1 - Type1 NSSA external, N2 - Type2 NSSA external,
       ABR - Area Border Router, ASBR - Autonomous System Border Router
=====
OSPF network routing table =====
N  172.16.2.0/24      [210] area: 0.0.0.0
                           via 172.16.10.1, uplink-634
                           via 172.16.13.1, uplink-611
N  172.16.3.0/24      [110] area: 0.0.0.0
                           via 172.16.10.1, uplink-634
N  172.16.4.0/24      [110] area: 0.0.0.0
                           via 172.16.13.1, uplink-611
N  172.16.5.0/24      [210] area: 0.0.0.0
                           via 172.16.10.1, uplink-634
                           via 172.16.13.1, uplink-611
N  172.16.6.0/24      [210] area: 0.0.0.0
                           via 172.16.10.1, uplink-634
                           via 172.16.13.1, uplink-611
N  172.16.10.0/31     [10] area: 0.0.0.0
                           directly attached to uplink-634
N  172.16.11.0/31     [110] area: 0.0.0.0
                           via 172.16.10.1, uplink-634
N  172.16.12.0/31     [110] area: 0.0.0.0
                           via 172.16.13.1, uplink-611
N  172.16.13.0/31     [10] area: 0.0.0.0
                           directly attached to uplink-611
N  172.16.20.0/31     [310] area: 0.0.0.0
                           via 172.16.10.1, uplink-634
                           via 172.16.13.1, uplink-611
```

```
SRV-EDGE-01(tier0_sr)> get ospf route
Codes: R - Router, N - Network, D - Discard,
       IA - Inter Area, E1 - Type1 external, E2 - Type2 external,
       N1 - Type1 NSSA external, N2 - Type2 NSSA external,
       ABR - Area Border Router, ASBR - Autonomous System Border Router
=====
OSPF router routing table =====
R  3.3.3.3              [310] area: 0.0.0.0, ASBR
                           via 172.16.10.1, uplink-634
                           via 172.16.13.1, uplink-611
R  10.10.10.10          [10] area: 0.0.0.0, ASBR
                           via 172.16.10.1, uplink-634
R  11.11.11.11          [10] area: 0.0.0.0, ASBR
                           via 172.16.13.1, uplink-611
R  20.20.20.20          [210] area: 0.0.0.0, ASBR
                           via 172.16.10.1, uplink-634
                           via 172.16.13.1, uplink-611
R  21.21.21.21          [210] area: 0.0.0.0, ASBR
                           via 172.16.10.1, uplink-634
                           via 172.16.13.1, uplink-611
R  100.100.100.100      [110] area: 0.0.0.0, ASBR
                           via 172.16.10.1, uplink-634
                           via 172.16.13.1, uplink-611
R  172.16.12.0           [110] area: 0.0.0.0, ASBR
                           via 172.16.10.1, uplink-634
                           via 172.16.13.1, uplink-611
R  172.16.22.0           [310] area: 0.0.0.0, ASBR
                           via 172.16.10.1, uplink-634
                           via 172.16.13.1, uplink-611
```

Useful commands

```
SRV-EDGE-01(tier0_sr)> get bfd-config
Wed Feb 03 2021 UTC 21:21:21.373
Logical Router
UUID          : 05ce9bec-4881-41c7-ac5b-1948654fae74
vrf           : 40
lr-id         : 202
name          : SR-Tier0-Tenant01
type          : PLR-SR

Global BFD configuration
  Enabled      : True
  Min RX Interval: 500
  Min TX Interval: 500
  Min RX TTL     : 255
  Multiplier    : 3

Port          : fed124b6-9cbb-4ed9-b712-cf1e776b2da3

Session BFD configuration

  Source        : 172.16.10.0
  Peer          : 172.16.10.1
  Enabled       : True
  Min RX Interval: 500
  Min TX Interval: 500
  Min RX TTL     : 255
  Multiplier    : 3

Port          : f0d9d25a-c428-4f8d-8692-0bc1b577fbc6
```

```
SRV-EDGE-01(tier0_sr)> get bfd-sessions
Wed Feb 03 2021 UTC 21:21:47.761
BFD Session
Dest_port          : 3784
Diag               : No Diagnostic
Encap              : vlan
Forwarding         : last true (current true)
Interface          : f0d9d25a-c428-4f8d-8692-0bc1b577fbc6
Keep-down          : false
Last_cp_diag       : No Diagnostic
Last_cp_rmt_diag  : No Diagnostic
Last_cp_rmt_state : up
Last_cp_state      : up
Last_fwd_state     : UP
Last_local_down_diag : No Diagnostic
Last_remote_down_diag : No Diagnostic
Last_up_time       : 2021-02-03 18:38:58
Local_address      : 172.16.13.0
Local_discr        : 3959728667
Min_rx_ttl         : 255
Multiplier         : 3
Received_remote_diag : No Diagnostic
Received_remote_state : up
Remote_address     : 172.16.13.1
Remote_min_rx_interval : 500
Remote_min_tx_interval : 500
Remote_multiplier  : 3
Remote_state       : up
```

OSPF

OSPF vs BGP

OSPFv2

Link State routing protocol (LSA flooding).

No support with IPv6. Must run BGP with IPv6 AF or static routes.

Dijkstra algorithm is computed on ALL router of an area every time there is a change in the area.

OSPF is very common in enterprise networks.

Support of BFD (BM: 50ms / VM: 500ms)

VRF / Federation **NOT** supported

BGP (recommended)

BGP updates only sent between BGP Peers.

One protocol for both IPv4 and IPv6 (AF)

BGP is very flexible (route-maps/set actions/communities/Filtering/Summary).

BGP is very easy to troubleshoot (Best path algorithm / advertised routes)

Support of BFD (BM: 50ms / VM: 500ms)

VRF / Federation Supported

Richer feature Set than OSPFv2 for NSX-T



What's New in NSX-T 3.1.1

NVDS to VDS

PM: Aditya Vikram Mukherjee and Sonam Sinha

TPM: Francois Tallet

February 2021

NVDS to VDS Upgrade

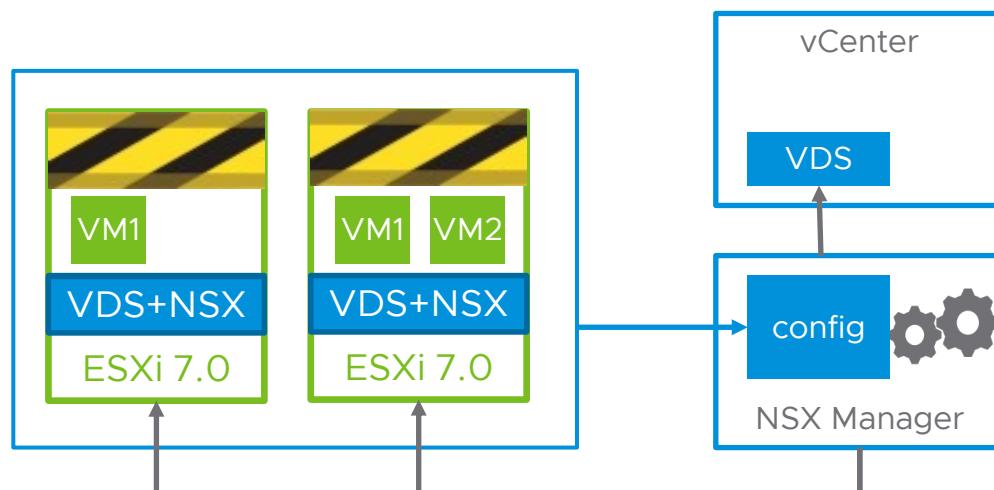
NSX-T 3.1.1

“Day 2” Switch Migrator Tool

Tool introduced in NSX-T 3.0.2

Migration entirely handled by the NSX Manager

Can be started via API or NSX Manager CLI



1. Do a pre-check and generate a configuration
2. Create a VDS in vCenter
3. NSX Manager coordinates the NVDS→VDS upgrade of each and every transport node

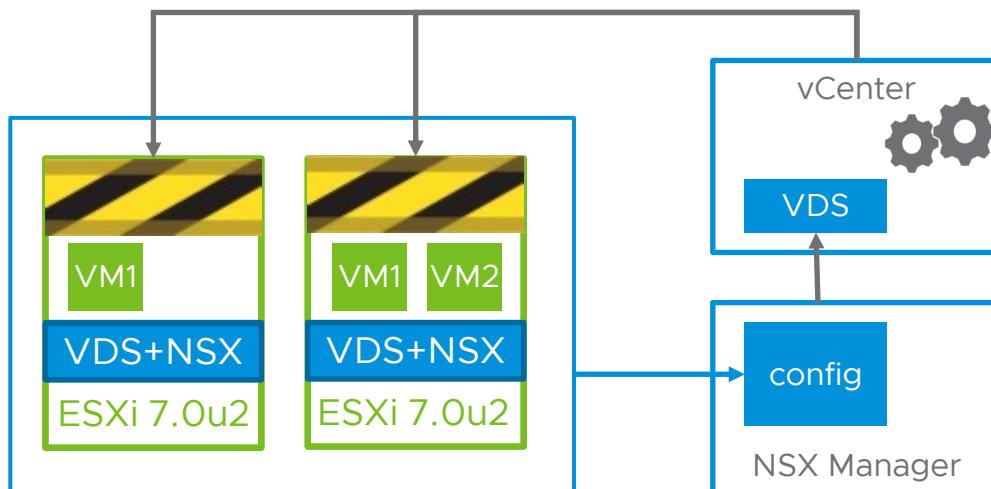
NVDS to VDS Upgrade

“Day 0” Switch Migrator Tool

NSX-T 3.1.1

NVDS→VDS Migration performed during the vSphere upgrade

Benefit: NVDS→VDS migration does not introduce additional downtime



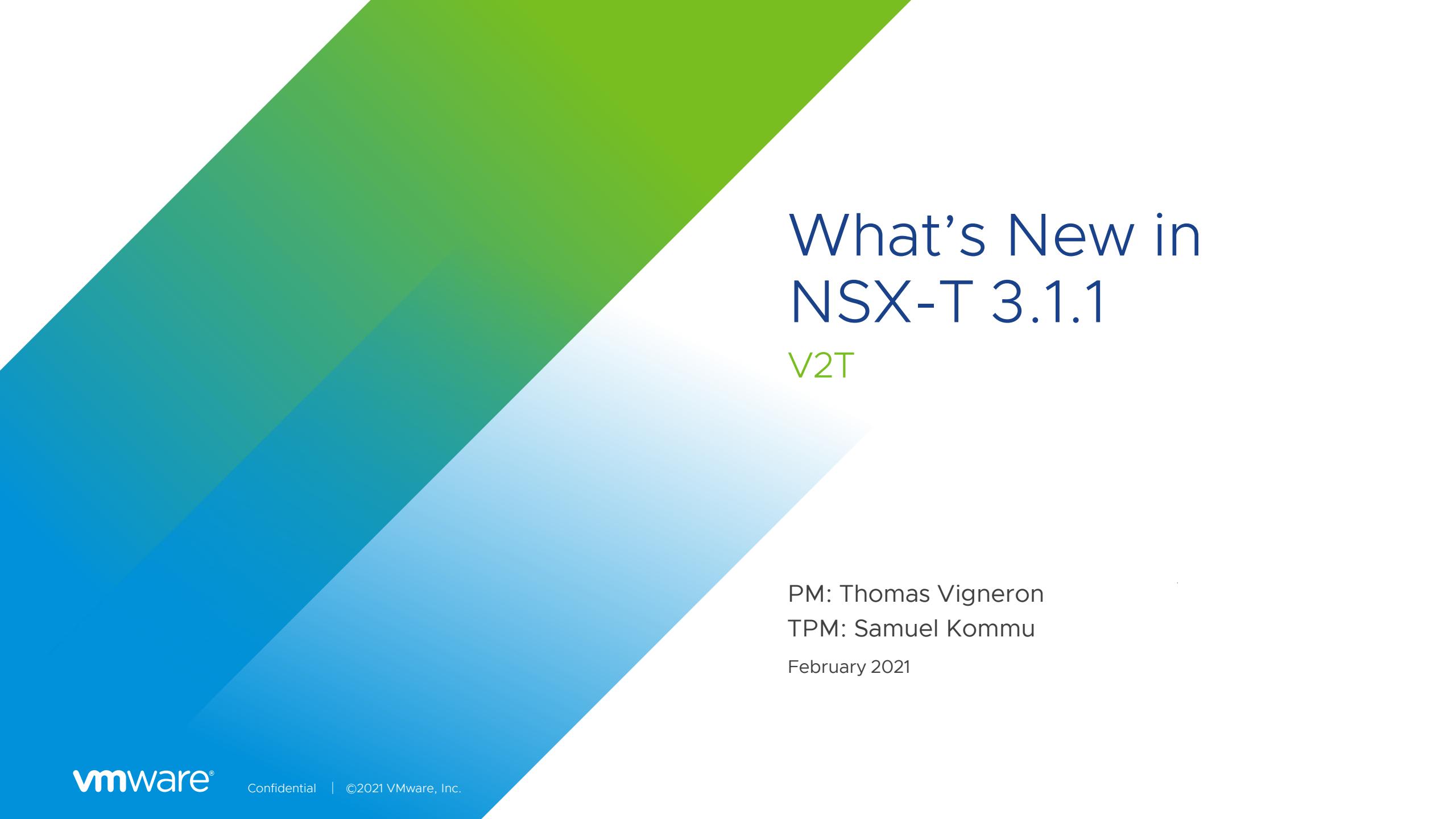
First part of the procedure performed by NSX manager

- NSX-T 3.1.0 triggered via API only
- NSX-T 3.1.1 introduces an NSX UI

1. Do a pre-check and generate a configuration
2. Create a VDS in vCenter
3. vCenter coordinates the NVDS→VDS upgrade and the ESXi upgrade of each and every transport node

Second part of the procedure is performed by the VUM (vSphere Upgrade Manager) in vCenter.

Will be available when upgrading to vSphere 7.0u2



What's New in NSX-T 3.1.1

V2T

PM: Thomas Vigneron

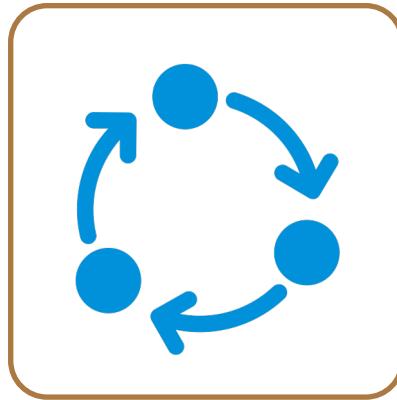
TPM: Samuel Kommu

February 2021

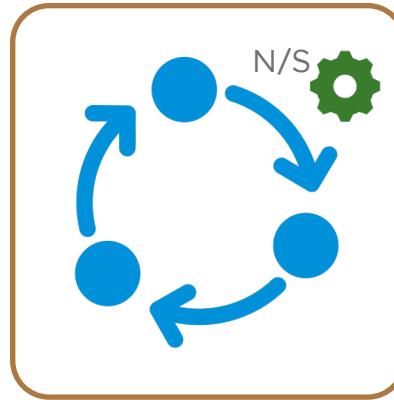
Migration Coordinator

NSX-T 3.1.1

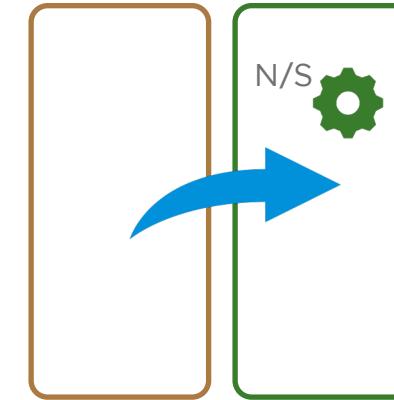
One Tool – Many Options



Use Same HW
Migrate Everything



Use Same HW
Custom NSX-T Design (N/S)
Migrate DFW, Workloads



Use New HW
Custom NSX-T Design (N/S)
Migrate DFW

← In-Place →

← Lift and Shift →

Resources: <https://vault.vmware.com/group/nsx/v2t-migration-t>

Migration Coordinator – Lift and Shift via GUI

NSX-T 3.1.1

One Tool – Many Options

The screenshot shows the NSX-T Management interface under the 'System' tab, specifically the 'Migrate' section. It displays several migration modes:

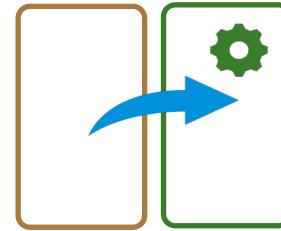
- STANDARD MIGRATION MODES:**
 - NSX for vSphere:** Shows a 'GET STARTED' button and a diagram of two nodes connected by a double-headed arrow. A blue box highlights this section with the text "In-Place (Everything)".
 - vSphere Networking:** Shows a 'GET STARTED' button and a diagram of a single node with a gear icon.
 - NSX for vSphere with vRealize Auto...:** Shows a 'GET STARTED' button and a diagram of two nodes connected by a double-headed arrow.
- ADVANCED MIGRATION MODES:**
 - Edge Cutover:** Shows a 'GET STARTED' button and a diagram of a single node with a gear icon.
 - Distributed Firewall:** Shows a 'GET STARTED' button and a diagram of two nodes connected by a double-headed arrow. A blue box highlights this section with the text "Lift and Shift".
 - Distributed Firewall, Host And Work...**: Shows a 'GET STARTED' button and a diagram of two nodes connected by a double-headed arrow. A blue box highlights this section with the text "In-Place (DFW, Hosts and Workload)".

A callout bubble points to the "vRA (*8.3)" logo in the top right corner.

Annotations on the screen include:

- "In-Place (Everything)" pointing to the NSX for vSphere card.
- "VCF Specific Use Case" pointing to the Edge Cutover card.
- "Lift and Shift" pointing to the Distributed Firewall card.
- "Custom NSX-T Design (N/S)" pointing to the Distributed Firewall, Host And Work... card.

Demo



Migration Coordinator - Lift and Shift

vSphere - Dashboard x NSX x +

vcsa-01a.corp.local/ui/#?extensionId=com.vmware.vshield.plugin.common.networksecurity.dashboardHome.navigateViewHTML

HOL Admin RegionA vCenter - Region A NSX-T Manager vRealize Log Insight Customer DB App Finance DB App HR DB App 1-Arm LB Customer...

vm vSphere Client Menu Search in all environments C ? Administrator@VSPHERE.LOCAL

Networking and Security

Dashboard

Overview System Scale

NSX Manager: 192.168.110.42 | Standalone

System Overview

Fabric Status

Host Preparation Status 4 Clusters
Unprepared clusters 2

Host Communication Channel Status 3 Hosts
No errors or warnings.

Host Notifications ①

No errors or warnings.

Service Deployment Status ①

No errors or warnings.

System Scale

Alerts: 0
Warnings: 2

Firewall Publish Status 3 Hosts
No errors or warnings.

Logical Switch Status 8 Logical Switches
No errors or warnings.

Backup Status

Backup schedule: ⚠️ FTP Server not configured
Last backup status: ⚠️ No record found

Edge Notifications ①

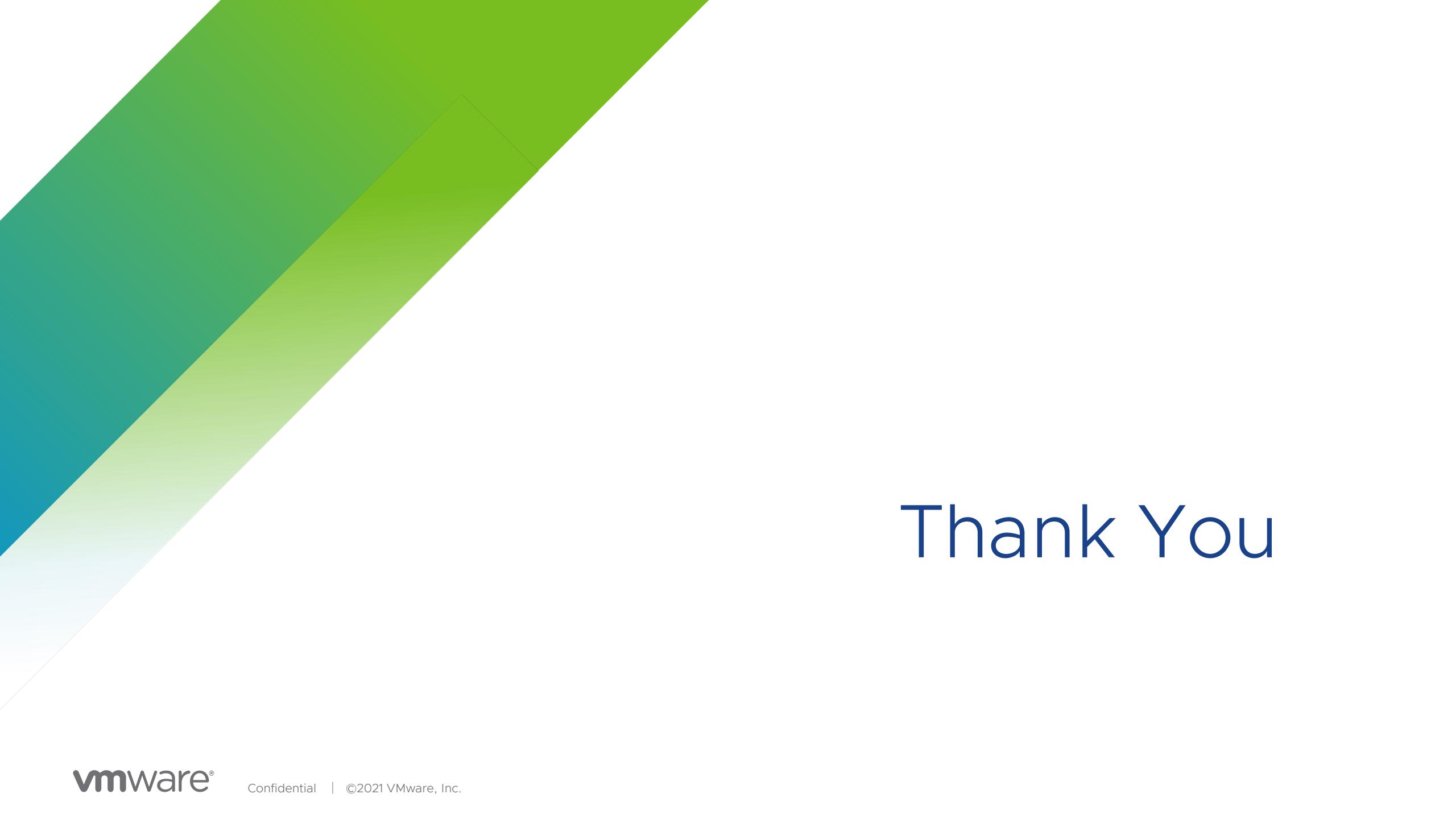
No errors or warnings.

Tools

Flow Monitoring: ⚠️ On
Endpoint Monitoring: Off

Recent Tasks Alarms

This screenshot shows the vSphere Client interface for NSX Networking and Security. The left sidebar navigation bar includes links for Installation and Upgrade, Logical Switches, NSX Edges, Security (with Firewall selected), Groups and Tags, Tools (Flow Monitoring, Traceflow, Packet Capture, Support Bundle, IPFIX), and System (Users and Domains, Events). The main dashboard displays various system status cards: System Overview, Fabric Status, Host Notifications, Service Deployment Status, System Scale, Firewall Publish Status, Logical Switch Status, Backup Status, Edge Notifications, and Tools. The Firewall Publish Status card indicates 3 hosts with no errors or warnings. The Logical Switch Status card shows 8 logical switches with no errors or warnings. The Backup Status card notes an FTP server is not configured and has no backup records. The Tools section shows Flow Monitoring is on and Endpoint Monitoring is off. The Firewall Publish Status card also lists 3 hosts.



Thank You