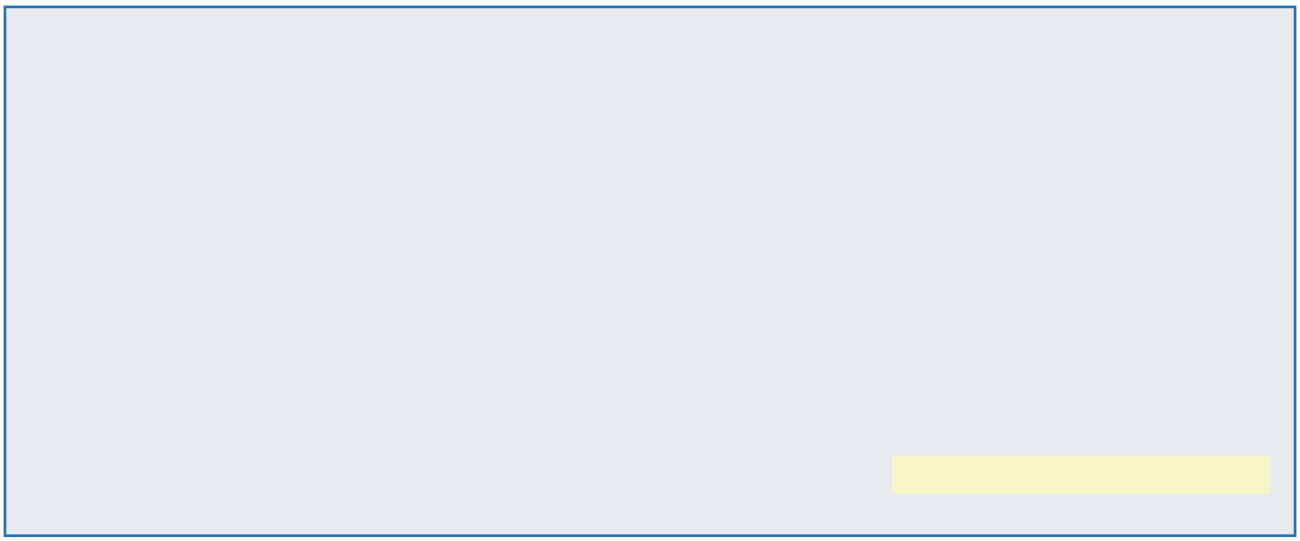
Table of Contents

Introduction

The guide describes how to deploy a wired network access with ubiquitous capabilities that scale from small

Deployment Details



Cisco Catalyst 3650 Series and Catalyst 3850 Series Switches are □xed-port, stackable, 10/100/1000 Ethernet switches, with PoE+ and non-power-supplying versions, which provide enhanced switching performance and resiliency through StackWise-160 (Cisco Catalyst 3650) or StackWise-480 and StackPower technologies (Cisco Catalyst 3850), with Flexible NetFlow capabilities on all ports.

- Cisco Catalyst 3650 stacking is implemented with an optional stacking module. Switches stack together us-
  - -

Configuring the Access Layer

1. Configure the platform
2. Configure LAN switch universal settings
3. Configure access switch global settings
4. Configure client connectivity
5. Connect to distribution or WAN router

Step 2: Set EtherChannels to use the traffic source and destination IP address when calculating which link to send the traffic across. This normalizes the method in which traffic is load-shared across the member links of the EtherChannel. This design uses EtherChannels extensively because of their resiliency capabilities. For this platform choice in this deployment layer, choose the following load-balancing option.

```
port-channel load-balance src-dst-mixed-ip-port
```

Step 3: For each platform, define two macros that you will use in later procedures to apply the platform-specific QoS configuration. This makes consistent deployment of QoS easier.

Tech Tip

```
    bandwidth remaining percent 1
 class class-default
    bandwidth remaining percent 25
    dbl
!
macro name AccessEdgeQoS
 auto qos voip cisco-phone
@
!
macro name EgressQoS
 service-policy output 1P7Q1T
```

Step 5: Enable the recovery mechanism to allow ports disabled as a result of errors to automatically clear the

Step 9:

Step 6: Con□gure the IPv6 First Hop Security global policy for host ports. This global policy is referenced by the access-layer port con□guration to intercept and drop IPv6 router advertisements from connected devices. Blocking the advertisements mitigates intentional and unintentional denial-of-service attacks and man-in-the-middle

Step 3:

Step 10:

```
  no shutdown
!
ip default-gateway 10.4.15.1
!
ip dhcp snooping vlan 100,101
no ip dhcp snooping information option
ip dhcp snooping
ip arp inspection vlan 100,101
!
spanning-tree portfast bpduguard default
!
ipv6 nd raguard policy HOST_POLICY
  device-role host
!
interface range
```

Example: Connected to WAN Router at a small site

```
  ip arp inspection limit rate 100
  ip dhcp snooping limit rate 100
  ip verify source
  ipv6 nd raguard attach-policy HOST_POLICY
  macro apply AccessEdgeQoS
!
! Next QoS Command for Cisco Catalyst 2960-X
mls qos queue-set output 1 threshold 3 100 100 100 3200
```

Procedure 5 Connect to distribution or WAN router

Access layer devices can be one component of a larger LAN and connect to a distribution switch, or, in the case of a small remote site, might be the only LAN device and connect directly to a WAN device. Unless the access layer device is a single fixed configuration switch connecting to a WAN router, Layer 2 EtherChannels are used to interconnect the devices in the most resilient method possible.

When using EtherChannel, the member interfaces should be on different switches in the stack or different modules in the modular switch for the highest resiliency.

The physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel interface. This allows for minimal configuration because most of the commands entered to a port-channel interface are copied to its members' interfaces and do not require manual replication. erdGraphi0 MC09>B

In the next step, you mitigate VLAN hopping on the trunk for switch-to-switch connections.

Example: Option 1, with LACP

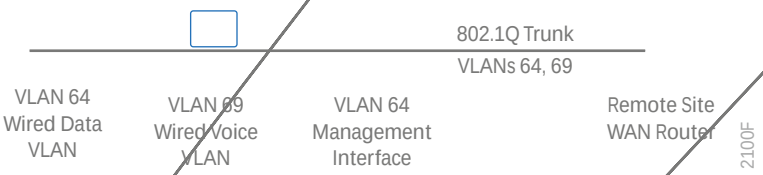
```
spanning-tree portfast trunk
logging event link-status
logging event trunk-status
load-interval 30
no shutdown
```

If the interface type is not a port-channel, you must configure additional commands switchport and macro apply EgressQoS on the interface.

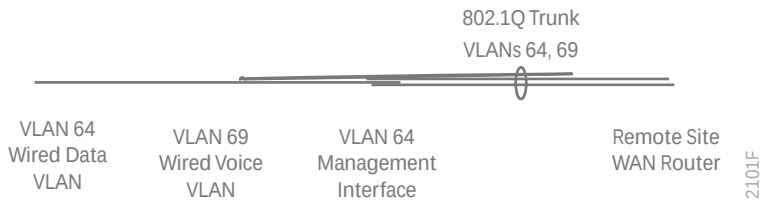
Step 3: Save the running configuration that you have entered so it will be used as the startup configuration file when your switch is reloaded or power-cycled.

```
copy running-confg startup-confg
```

Example: Option 2, without EtherChannel



Example: Option 2, with EtherChannel



Simpli□ed Distribution Layer Deployment

DISTRIBUTION LAYER PLATFORMS

You can use multiple platforms to deploy the simpli□ed distribution layer design. Physically, the distribution layer

- Provides Stateful Switch-Over (SSO) to synchronize infrastructure and forwarding state between chassis, along with Non-Stop Forwarding (NSF) for graceful-restart of L3 routing protocols, in the event of a chassis failure. Also allows Enhanced Fast Software Upgrades (EFSU) with In-Service Software Upgrades (ISSU) for minimizing downtime for system upgrades.
-

Figure 5 VSS domain

This design uses the Fast-Hello (VSLP) link for dual-active detection in this stage. Enhanced PAgP can be added to the design when bringing up PAgP EtherChannel links. The Fast-Hello link is a Gigabit Ethernet interface on each VSS switch chassis and connects them together (similar to a VSL connection) in a back-to-back fashion. This link does not require high bandwidth because it is only a detection link with control plane hellos on it.

Figure 6 VSLP

Option 2:

```
random-detect dscp 26 percent 90 100
```

Option 4:

Procedure 2 Con□gure LAN switch universal settings

In this design, there are features and services that are common across all LAN switches, regardless of the type of platform or role in the network. These are system settings that simplify and secure the management of the solution.

Option 1:

```
ntp source Loopback 0
!
router eigrp LAN
 address-family ipv4 unicast autonomous-system 100
  af-interface default
   passive-interface
  exit-af-interface
  network 10.4.0.0 0.1.255.255
  eigrp router-id 10.4.15.254
  eigrp stub summary
  nsf
 exit-address-family
!
```

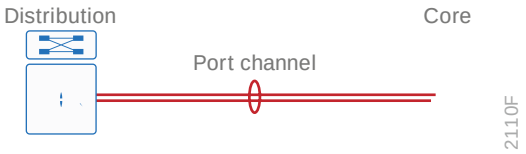
```
no passive-interface Port-channel30
network 10.4.0.0 0.0.15.255 area 1
network 10.4.40.0 0.0.0.255 area 0
```

Option 1:

```
interface GigabitEthernet 2/1/2
  description Link to Access Switch Port 4
!
interface range GigabitEthernet 1/1/1, GigabitEthernet 2/1/1, GigabitEthernet
1/1/2, GigabitEthernet 2/1/2
  switchport
  channel-protocol lacp
  channel-group 10 mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  load-interval 30
  macro apply EgressQoS
  no shutdown
!
interface Port-channel 10
  description EtherChannel Link to Access Switch
  switchport trunk native vlan 999
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 100,101,115
  switchport mode trunk
  load-interval 30
  no shutdown
!
interface vlan 100
  ip address 10.4.0.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode
!
interface vlan 101
  ip address 10.4.1.1 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim sparse-mode
!
interface vlan 115
  ip address 10.4.15.1 255.255.255.128
  ip pim sparse-mode
```

Step 2: If the routing protocol you are using is OSPF, you add the router neighbor authentication con□guration to

Example: Distribution to Core PortChannel con□guration–OSPF



LAN CORE LAYER

Appendix B: Changes