LAN Baseline Architecture Branch Office Network Reference Design Guide

This document provides guidance on how to design a local area network (LAN) for a Business Ready Branch or autonomous Business Ready Office where corporate services such as voice, video, and data are converged onto a single office network.

Because of the numerous combinations of features, platforms, and customer requirements that make up a branch office design, this version of the design guide focuses on various LAN designs for voice and data services. This document also includes design guidance on the LAN side of the office network using features such as 802.1x and Cisco Catalyst Integrated Security.

Contents

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Hardware and Software Options

This section provides various hardware and software options for the LAN portion of the network. The hardware and software options are categorized based on multilayered branch architecture.

Access Switches

Factors to consider when choosing access layer switches include the following:

- Spanning tree requirements
- Layer 2 security features such as Cisco Integrated Security Features (CISF) requirements
- Support for private virtual LANs (VLANs)
- Support for Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN)
- Quality of service (QoS) requirements
- Power Over Ethernet (PoE) requirements
- Authenticator capabilities for 802.1x authentication

Although the recommended branch architecture is loop-free, rapid spanning tree is the recommended protocol to be enabled on the switch. All the access switch platforms support multiple spanning tree protocols. However, by default, the IEEE 802.1D protocol is enabled. To take advantage of the rapid convergence, deploy the access switches that support 802.1s/1w and Rapid Per-VLAN Spanning Tree Plus (RPVST+).

CISF provides the necessary Layer 2 security for the access layer, including port security, dynamic ARP inspection, and other features.

Private VLANs (PVLANs) provide the isolation required between clients or end users. Catalyst 3750 and 3560 platforms support full PVLAN support. Most other low-end platforms support only a subset of PVLAN features. If full PVLAN support is desired, only limited options exist.

SPAN and RSPAN are useful features for troubleshooting, and can also provide intrusion detection services (IDS) when used with IDS appliance devices. Upper-end access switches such as the Cisco 3750 and 3560 support SPAN and RSPAN without losing a physical port. However, on low-end access switches such as the Cisco Catalyst 29xx, the configuration requires that one of the ports be used as a reflector port, which becomes unusable for the end user.

QoS and policing requirements dictate the use of specific platforms. Certain platforms with low granular policing capabilities cannot be used when using QoS and policing to rate limit end-user traffic.

Most access switches provide features that can provide 802.1x authentication capabilities and guest VLAN capabilities, so this should not be concern when choosing an access switch.

Table 3 in the Appendix, page 44, lists all the platforms and the features supported.

Distribution Switches

Typically, a distribution switch operates at Layer 3 as well as Layer 2. The following features are important for the distribution switches:

- Cost considerations
- Spanning tree protocols
- PVLAN capabilities

- Routing protocols
- Policy-based routing
- VRF capabilities
- High availability
- Scalability

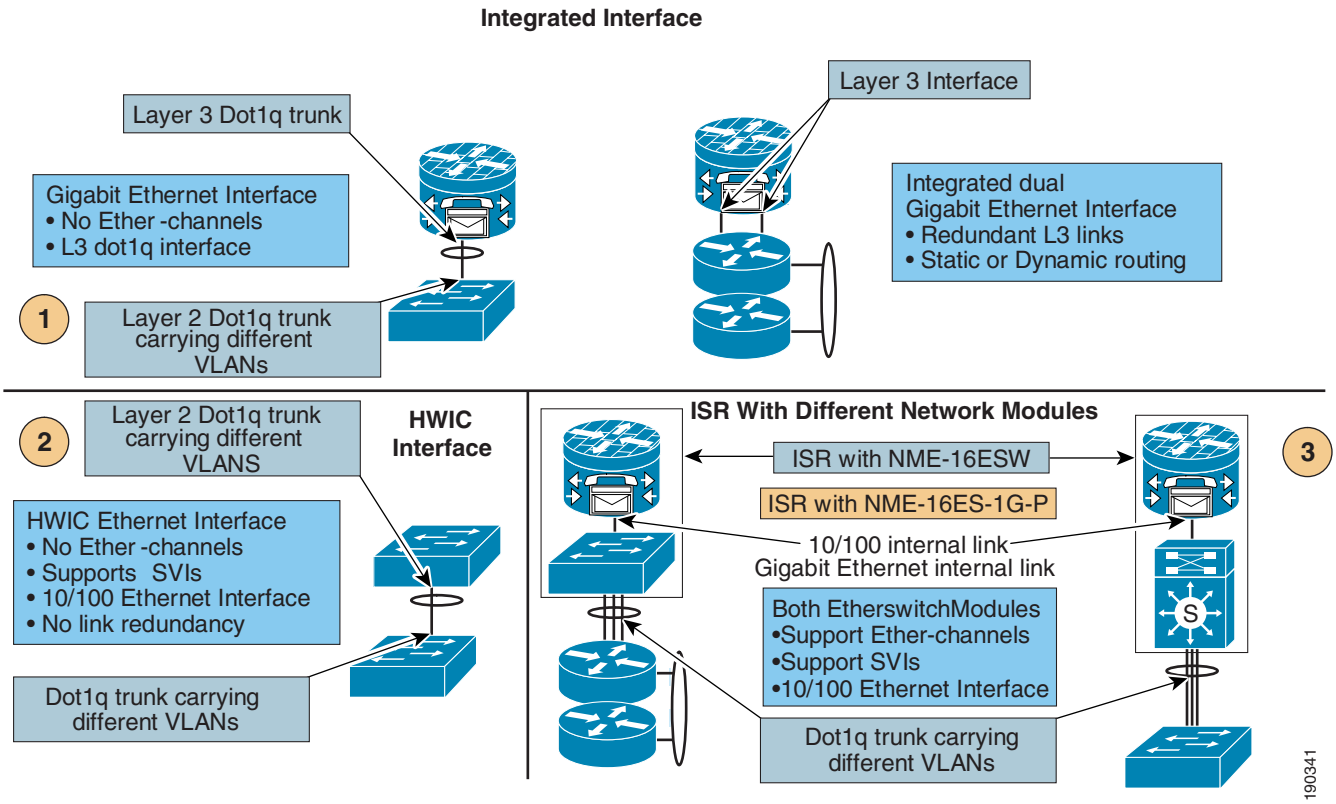
Integrating with the Edge Layer

The integrated services router (ISR) at the edge layer provides various voice and data services. This section provides detail of how the LAN can be integrated with the edge layer. Depending on the edge router, the following interfaces are available to integrate with the LAN:

- Integrated interfaces (10/100/1000)
- High-speed WAN Interface Card (HWIC) Ethernet 10/100 interfaces
- Network modules

Figure 1 provides details about these three ways of integrating with the edge.

Figure 1 Integrating with the Edge Layer



Each of the options except HWIC can be used in various ways, based on the topology (Layer 2 or Layer 3).

The 10/100/1000 integrated interface on the ISR has the following characteristics:

- Does not support Switched Virtual Interfaces (SVIs)
- Cannot be channeled with other 10/100/1000 integrated interfaces on the ISR
- Can be used as a trunk for multiple VLANs (different L3 subnet)
- Redundant links to the distribution with static and dynamic routing

The HWIC Ethernet interface is not recommended in a multi-layered architecture for the following reasons:

- No support for channeling
- Supports only 10/100 interfaces which cannot be used for uplinks

The third option shown in Figure 1 uses an integrated network module, or an integrated EtherSwitch Services Module. Table 1 provides a brief description of the capabilities of both the network modules.

T

Table 1 Comparison of Two Network Modules

NME-16ESW	Services Module (NME-16ES-1G-P)
• 10/100 internal interface to the ISR	• 10/100/1000 internal interface to the ISR
• Does not support 802.1s/w	• Supports 802.1s/w
• Supports SVCs, channels	• Supports SVCs and channels
• Can be integrated at Layer 2 or Layer 3 with the internal interface	• Can be integrated at Layer 2 or Layer 3 with the internal interface
• 802.1x CLI is not consistent with Cisco Catalyst switches	• 802.1x CLI is consistent with Cisco Catalyst switches
• Advanced QoS features of Cisco Catalyst 3750/3650 are not supported	• Advanced QoS features of Cisco Catalyst 3750/3650 are supported
• Cannot be stacked with external Catalyst 3750 switches	• Can be stacked with external Cisco Catalyst 3750 switches

Note The services module comes in various form factors with and without stacking capability. NME-16ES-1G-P is one example of services module.

Because of the support of 802.1s/w on the services module and other advanced features, it is the preferred module because it provides multiple options of connectivity without compromising high availability and scalability.

Details concerning the options of integrating the access or distribution are provided in later sections.

Branch LAN Design Options

Based on the number of users in the branch, three design models can be used, each of which offers a certain amount of scalability. The choice of models is affected by requirements such as high availability, because some of the interfaces on the edge router do not support EtherChannels. If a server farm must be supported in the branch, the design must support the required port density to connect the small server farms and to meet the additional DMZ requirements. High availability, scalability, and advanced services add to the cost of the infrastructure. Layer 2 and Layer 3 switches do provide some alternatives to which

software images can be used to keep the cost low while still providing high availability and scalability. Also, the infrastructure can be reused to migrate to advanced services if required without having to redesign.

Another consideration for the LAN design is the oversubscription at the access layer. Erlang suggests an oversubscription ratio of 3:1 for voice over IP (VoIP). For data networks, no rule dictates how data networks can be efficiently oversubscribed. Oversubscription ratios really depend on the end user utilization (applications being used). Studies done by the industry and academic institutions suggest that the network is highly underutilized at the edge of the network. The bursty nature of the data traffic and the underutilization of the Ethernet suggest that networks can be oversubscribed intelligently. Queuing and scheduling mechanisms in the end devices can be effectively used to handle congestion at the edge of the network, and at the access layer in the case of the branch and campus network. For more information, see the following URL: http://www.cisco.com/en/US/partner/products/hw/switches/ps5206/products_configuration_guide_chapter09186a008039ed19.html#wp1284809

The oversubscription requirements can be different if a server farm must be supported at the branch office. Typically, the server farm has better utilization of the Ethernet bandwidth, and lower oversubscription ratios are recommended. Again, no predefined ratios can be used in such cases. The oversubscription depends on the applications and the traffic to and from the server farm.

Manageability of the branch network should be simple enough to deploy and maintain. The architecture should enable the management of the networks and yet meet all the design criteria.

The requirements are different for different-sized branch offices. Based on the discussions above, the following lists the basis for LAN design at the branches:

- Number of users
- Cost
- High availability
- Scalability
- Security
- Server farms and DMZ requirements
- Management

The number of users supported is really limited by the physical number of ports available. Besides the scalability considerations, the high availability requirements point to various design models as well. Based on the number of users, the branch office is categorized as follows.

- Small office—Up to 50 users
- Medium office—Between 50 and 100 users
- Large office—Between 100 and 200 users

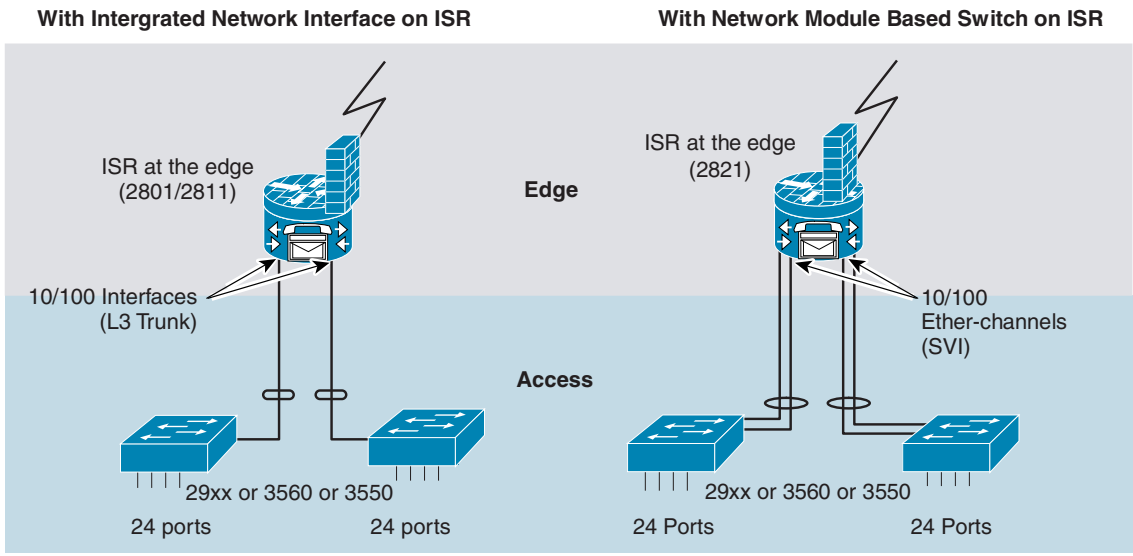
Based on this classification, the various design models are described in the following sections. High availability, scalability, and migration to advanced services requirements also influence the model adopted.

Small Office Design

Figure 2 provides two models that can be used for a small office design to support up to 50 users. The first option, called a trunked topology, uses the integrated network interface on the Cisco ISR. There is no link redundancy between the access switch and the ISR. The second option, called the EtherChannel

topology, uses a network module-based switch on the ISR to provide link redundancy to the access layer. Note that the second option uses the Cisco 2811 ISR. If redundant links and higher bandwidth uplinks are required, only the second option can be used.

Figure 2 Small Office Design



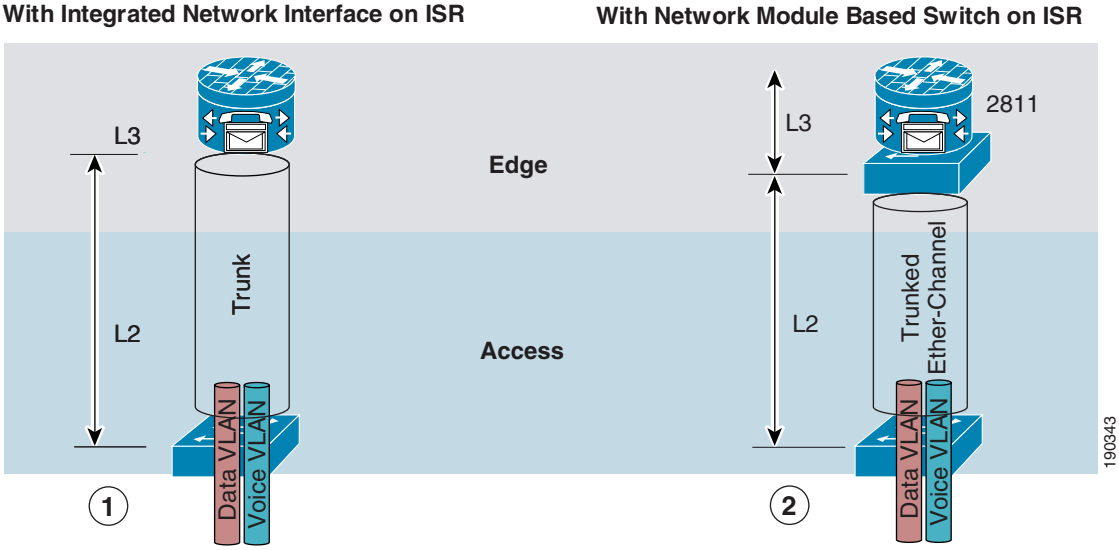
The Cisco 2801 ISR has a fixed configuration from an Ethernet connectivity perspective. The Cisco 2811 has several options that can be used in various ways. Table 2 summarizes the characteristics of the Fast Ethernet interfaces of the 2801 and 2811. The choice of the edge router also depends on the voice and VPN considerations which are not discussed in this document.

Table 2 Ethernet Interfaces of Cisco 2801 and Cisco 2811

Cisco 2801	Cisco 2811
Two integrated 10/100 interfaces	Two integrated 10/100 interfaces
Supports Layer 3 dot1q trunk	Supports Layer 3 dot1q trunk
No SVIs supported	No SVIs supported on integrated interfaces
No EtherChannels supported	Supports Ethernet HWIC module with the following characteristics: • 10/100 Interfaces • No EtherChannel support • Supports SVI • Single Fast Ethernet connects the HWIC module with the router internally • Supports a slot for network module • 16 port Ethernet switch module with support for SVIs and EtherChannels • Single Fast Ethernet connects the network module with the router • IDS module • Supports network-module with the following characteristics • 10/100 and 1000 depending on the type of network module used • Provides Etherchannel support • Ethernet Switch with support for SVIs and EtherChannels • Single GigabitEthernet connects the network module with the router internally • Supports only 802.1D Spanning Tree

The difference between a Cisco 2801 and a Cisco 2811 from LAN perspective is the support of a slot for a network module, as shown in Table 2. Figure 3 shows a logical diagram for the topologies.

Figure 3 Logical Topologies Diagram



The access switch supports Layer 2 services, and the Cisco ISR provides Layer 3 services. In both cases, the default gateway is on the ISR. With a 24-port access switch, this model supports up to 24 users per access switch. If PoE is desired for all the users on the access switch, see the product documentation to find out whether PoE is supported on all the ports of the access switch.

To keep the manageability simple, there are no loops in the topology. In option (2) for small office design, where the network module-based Ethernet switch is used, redundancy can be provided by EtherChannels. The switch icon represents the network module, as shown in option (2) of Figure 3. The ISR provides Layer 3 services such as DHCP, firewall, and NAT. As shown in Table 2, the connectivity between Ethernet network module and the ISR is via Fast Ethernet.

The Layer 2 domain requires a spanning tree protocol. Note that there are no Layer 2 loops in this design, and that spanning tree must be enabled and configured to protect the network from any accidental loops. The recommended spanning tree protocol is Rapid PVST+ for all Layer 2 deployments in a branch office environment. In the current topology (option 2 in Figure 3), the network module-based Ethernet switch in the ISR is configured as the primary root. If the primary root fails, there is no redundant path for the traffic. ISR high availability is currently being investigated, and the design guidance will be provided in the near future. The complexity arises because of the CallManager Express and Cisco Unity Express on the ISR. Note also that in this topology, the network module-based Ethernet switch in the ISR does not support enhanced spanning tree protocol. However, the EtherSwitch Services Module supports enhanced spanning tree protocol in the network module, and the design details are covered in the Large Branch Office Design section of this guide. The Ethernet Switch Module (NM-16ESW) running 802.1D spanning tree interoperates with the access switches running enhanced spanning tree. The spanning tree configuration details are provided in a later section of this guide.

The traffic between access switch and the ISR is not load balanced on a per-packet basis. Rather, the load balancing is done based on the source or destination MAC address. Packets originating from a specific address always use the same link of the channel at all times. The switch provides a choice of source or destination address to be used for load balancing. Cisco recommends using the source MAC address for traffic originating from the access switch, and to use the destination MAC address for traffic originating from the ISR.

The default gateways for the clients are configured on the ISRs. There is a default gateway for each VLAN configured in the topology. All the Layer 3 configurations are done on the ISR. The access switches must be configured with an IP address for management purposes.

Scalability and High Availability

From a scalability perspective, the number of switches that can be deployed for end user connectivity is limited in option 1. With option 2, more access switches can be connected to the network module-based Ethernet switch. Scalability requirements to some extent are also met with this design.

The EtherChannels between the access switch and the switch module in the ISR supports high availability in relation to link failure, as well as load balancing the EtherChannel traffic.

Note The access switches cannot be connected to multiple network modules. Failure of the network module implies that there is no redundant path for the end users.

Another possible failure, although rare, is the internal link between the ISR and the network module. Because it is a bus, the link status is always up in case of interface failure or unidirectional link. Under such circumstances, there is no redundant path in the small office design.

Note For more information, see Large Office Design, page 13, which describes a redundant path in such failure scenarios using EtherSwitch Services Modules.

Security and Manageability

Although 802.1x is supported on the network modules, Cisco recommends using the access layer and the network modules to provide redundancy and scalability, because of the lack of implementation consistency (from a CLI perspective) with the Cisco Catalyst access switches. Layer 2 security is supported only on the Cisco EtherSwitch Service Module. To be able to scale and incorporate Layer 2 security into a branch LAN design, Cisco recommends using the access layer with Cisco Catalyst switches.

In addition to the security features, the Cisco EtherSwitch Services Module also supports 802.1s/w. The access layer switches, when used with the EtherSwitch Service Module, provide quick Layer 2 convergence if Layer 2 loops are present in the topology.

Note When the network grows, it might be necessary to move to a large-scale model, where 802.1s/w becomes important.

From a manageability standpoint, it is fairly straightforward to manage all the topologies. Having Cisco EtherSwitch Service Modules in the ISR provides additional benefits as discussed in the Large Office Design section.

Medium Office Design

The medium office topology is similar to the small office topology except that the edge router used is either a Cisco 2821 or Cisco 2851. Similar concepts are used for the design. Both the 2821 and 2851 support two integrated 10/100/1000 interfaces, which are L3 native. Both the 2821 and 2851 support one slot for a network module. To scale up to 100 users, the following options are available:

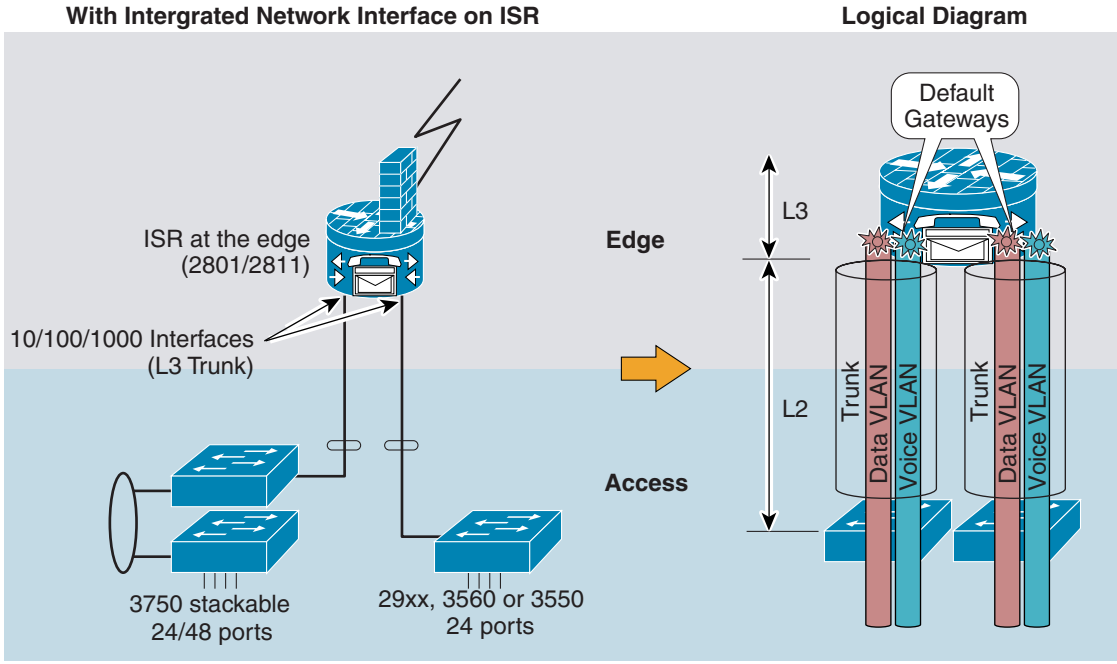
- Use higher port density access switch (48 port)
- Use the network module that supports up to 16 ports, and use EtherChannels to connect to the access switches

Although the 48-port access switch supports the required GigE interfaces, see the product documentation for inline power considerations. To scale up to 100 users, the second option provides the required scalability, in addition to providing high availability (link redundancy).

Note Only the Cisco 2851 supports the high-density 36-port network module. The Cisco 2821 supports only the 16-port network module.

Figure 4 shows the first of the two topologies that fit the medium office design.

Figure 4 Medium Office Design (Trunked Topology)



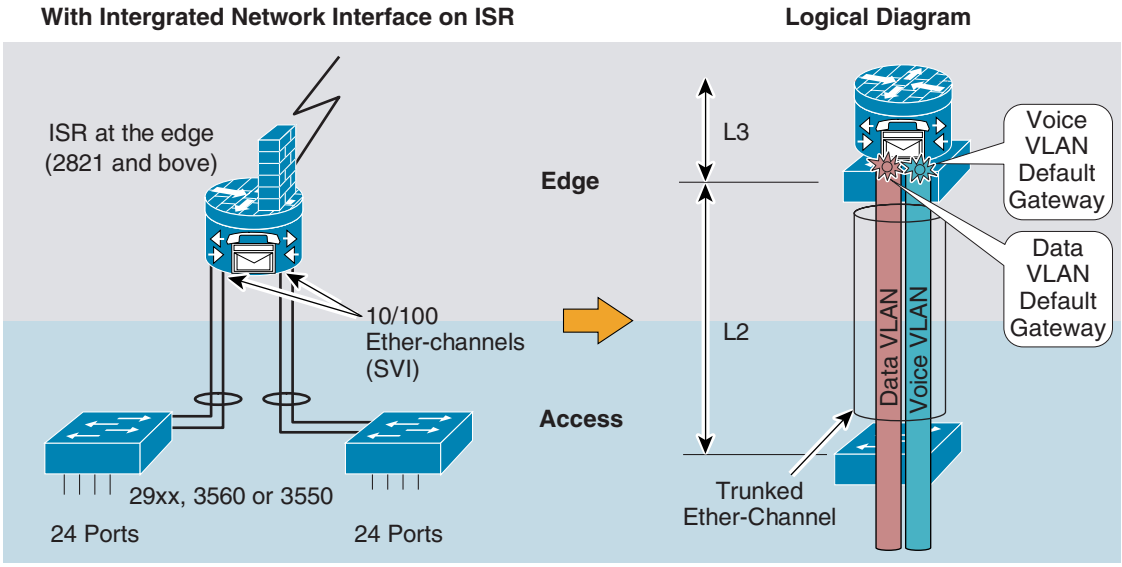
This topology uses the integrated 10/100/1000 interfaces as Layer 3 trunks. The 10/100/1000 interface provides the flexibility to use various access switches. The stackable Cisco Catalyst 3750 with a standard image or an IP base image can be used as the access switch to support 24/48 users per switch. Support for the number of users needing PoE depends on what is supported on the access switch. With two switches and 24 users per switch, the design can easily meet the medium office requirements. The users are grouped into two different subnets. As shown in Figure 4, there is always the option of using different access switches. To be able to meet the medium office requirements, using a stackable switch on two different 10/100/1000 interfaces is a good approach. The Catalyst 3750 supports all the access features that are available and is a good fit for a medium-sized office.

The default gateways for voice and data reside on two different dot1q sub-interfaces. Also with this model, the users coming in through a different access switch also reside on a different subnet on the second 10/100/1000 interface. With route summarization at the edge in mind, data and voice IP addressing can be subnetted to be contiguous on the two physical interfaces of the edge router.

There is no Layer 2 switch on the edge router, and there are also no loops in the topology. With this topology, there is no need to configure a Layer 2 topology. By default, spanning tree is enabled on all access switches, but there is no spanning tree configuration involved. However, it is important to follow a consistent access switch configuration so that if in the future a network module-based EtherSwitch is used in the edge router, only the EtherSwitch in the edge router needs to be configured as the root bridge.

Figure 5 shows the second option.

Figure 5 Topology for Medium Office Design (EtherChannel Topology)



This topology is similar to the small office design. In this topology, there is no need to subnet the traffic from different access switches. One default gateway for the data VLAN and one default gateway for the voice VLAN is all that is needed for this topology.

To be able to support the required number of users, the network module-based Ethernet switch becomes a bottleneck because the switch connects to the ISR CPU by a single 10/100 connection. Although this topology supports trunking and high availability from link failures, the bandwidth limitation between the network module switch and the ISR is a concern. Until the bandwidth limitation is relieved, this topology is not recommended with the existing 16-port network module. In addition to the bandwidth limitation, there is the loss of a slot that could have been used for intrusion detection.

With the topology in Figure 5, the network module-based Ethernet switch has to be configured as the root bridge. Although there are no Layer 2 loops, turning the spanning tree on provides protection against accidental loops. The Layer 2 recommendations are similar to a small office design. The NM-ESW16 and NM-ESW36 do not support Rapid Spanning Tree Protocol. The EtherSwitch in the edge router must run 802.1D Spanning Tree Protocol. The CPU on the edge router is involved in spanning tree; however, the access switches can be running the Rapid Spanning Tree, and it interoperates with 802.1D on the edge router. The edge router is the spanning tree root.

Scalability and High Availability

This design is almost identical to the small branch office. Deploying an integrated switch in ISR helps to achieve high availability and scalability. Access layer switches have to be used to scale up to the required number of users. As noted in the previous section, high availability is limited to link failures. Device failure (integrated switch failure) isolates a segment of the users. However, if high availability is one of the primary concerns, a model described in Large Office Design, page 13 can be used.

Security and Manageability

The discussion for the small branch office design applies also to the medium branch office design. Deploying the access layer switches helps in achieving a uniform perimeter design for the branch office design.

Large Office Design

A large office design is one step closer to a campus design. In addition to supporting more users, a large office might also need higher LAN switching capability if supporting a server farm (DMZ). Support for some of these services requires the use of appliance devices if higher throughput is required. To meet these requirements, a distribution layer is added to the small office or medium office topology by introducing a Layer 2/Layer 3 switch to provide the required LAN switching capabilities, port density, and flexibility to support additional appliances.

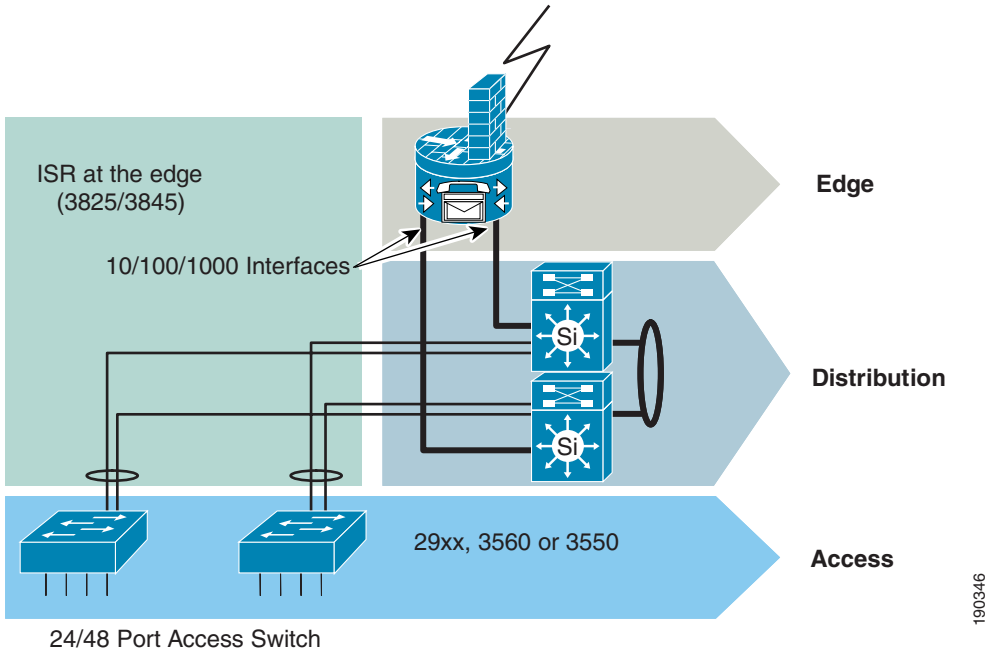
There are the following two options:

- Conventional design using external switches for the distribution layer
- Integrated routing and switching using integrated switching for the distribution layer

Conventional Design

Figure 6 shows a large office LAN topology. In this topology, a stackable switch (Cisco Catalyst 3750) is shown. The stackable distribution switch can be replaced by a Cisco Catalyst 4500 switch.

Figure 6 Large Office Network Topology



This LAN topology is highly available, scalable, and manageable. High availability requirements are met because link redundancy and device redundancy are built into the design. As shown in Figure 6, the EtherChannel is across the stack that provides redundancy for link as well as stack-switch failure. When

the solution was tested, the only support available was EtherChannel for cross stack switches. For high availability between the distribution and the edge layers, only redundant links can be used with both the IP base image and enhanced image. With the enhanced image, per-packet load balancing can also be configured. With the IP base image, two default routes can be configured with different metrics on the distribution layer.

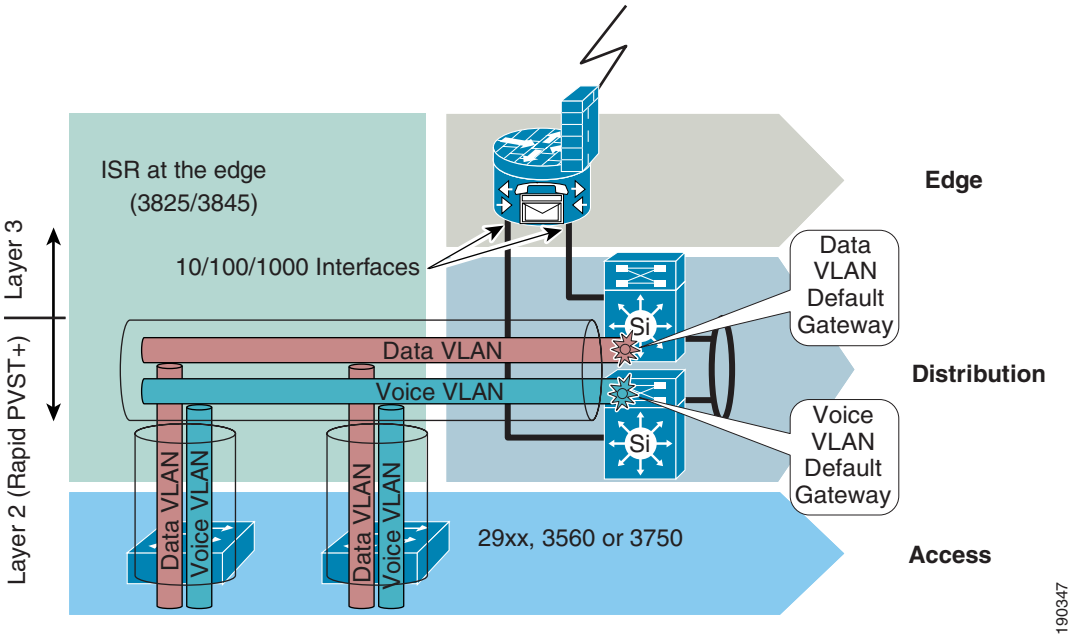
This design meets the scalability requirements as well. The port density of the stacked switches allows a number of access switches to be connected without compromising high availability. The distribution switch capacity can be increased by adding additional switches to the stack if required.

The distribution switches can run either standard/base image with static routing, or the enhanced images, which support more features including various routing protocols. With the standard image, some of the advanced features such as PVLAN, policy-based routing, and routing are not available. With this design, it is possible to add advanced services by using an enhanced image on the distribution switch.

To achieve high availability with a chassis-based solution (Cisco Catalyst 4500), a redundant supervisor and redundant power supply must be deployed. The chassis-based solution is not described in this document.

Figure 7 provides a logical view of a large branch office topology. The Layer 2 traffic for all VLANs terminates at the distribution layer. The distribution layer must run both Layer 2 and Layer 3 protocols. Layer 2 protocols provide connectivity to the access layer and Layer 3 provides connectivity to the distribution layer.

Figure 7 Logical Diagram of a Large Branch Office Topology



The distribution layer and the access layer switches are running RSTP. The distribution layer is the root bridge. Again, by using RSTP, there is no need to enable UplinkFast and BackboneFast. In addition to RSTP, additional features to protect against loops are enabled on the distribution and the access layers. For instance, RootGuard can be enabled on the distribution switch to protect against the claims as root of another switch.

If Cisco Catalyst 3560 and 3750 switches are used at the access layers, other Layer 2 security features such as DHCP Snooping, Dynamic ARP Inspection, and IP Source Guard can be enabled, which provides additional security measures. These features are available in the standard or IP base image. The configuration section provides detailed configuration information of all the features.

As mentioned in the previous sections, the distribution layer is a staging layer for a number of services at the branch office. The default gateways for all the VLANs at the access layer are configured on the distribution layer. Only the voice and data VLAN default gateways are shown in Figure 7. Other types of VLANs are the guest VLAN and WLAN VLANs.

Layer 3 integration with the edge layer can be provided by either static or dynamic routing. The interface between the distribution and the edge layers is provided by configuring Layer 3 interfaces and configuring static/dynamic routing based on requirements. As an alternate configuration, the router interface at the edge layer supports dot1q trunks as well. The interface between the edge and distribution can be a trunk if there is a requirement to tunnel the Layer 2 traffic to the edge layer to make use of the service running on the edge switch. Although this can be done, Cisco recommends providing clear traffic boundaries and maintaining the modularity.

Note Do not span VLANs across switches unless it is absolutely required.

Integrated Routing and Switching Design

With this design option, the distribution layer can be integrated in the ISR to provide an integrated routing and switching with the new Cisco EtherSwitch Service Modules. The Cisco EtherSwitch Service Modules provide the feature parity with Cisco Catalyst 3750 and can be installed into the ISR. These network modules are smaller versions of the Cisco Catalyst 3570 with its own CPU. These switches provide the ability to aggregate traffic from the end user clients. The network module makes it possible to collapse the distribution layer into the edge in a branch architecture.

Using the network modules has the following advantages:

- ISR and network modules are integrated into a single chassis
- Lower ISR CPU utilization if traffic is switched
- Provides a good integration point for the access layer into the edge
- Provides enterprise class services for Layer 2 and Layer 3
- Provides advanced security and QoS features with services modules

The network module comes in various configurations with and without inline power. From a design point of view, the network module can be used in all three branch designs: small, medium, and large. As mentioned above, the network module provides more benefits as compared to earlier designs. However, if the ISR can handle all the client traffic, and there is no need to make use of the added benefits either for cost or technical reasons, the designs mentioned in the previous sections can be used. This design meets the following guidelines:

- High availability
- Scalability
- Security
- Manageability

With these requirements and the various branch office sizes in mind, the integrated EtherSwitch service module design suits the requirements of a large branch office. Small- and medium-sized branch office design can also deploy integrated switching design models without having to deploy the access layer for scalability if the number of ports available can support the number of users.

Note Integrated switching in ISRs can be used without the access layer in the design for small- and medium-sized branch office networks if high availability is not a criteria. In such cases, only Layer 3 connectivity along with static routes can meet the requirements. Because such a configuration is straightforward, the design solution is not discussed.

The following designs are discussed for medium and large office designs:

- Dual EtherSwitch Service Module design
- Integrated stackable EtherSwitch Service Module design

Dual EtherSwitch Services Module Design

The dual EtherSwitch Service module design implies that the ISR being used is the Cisco 3845. The number of network modules supported in an ISR is provided in Table 2 of the following URL. http://www.cisco.com/en/US/partner/products/ps5855/products_qanda_item0900aecd8028d16a.shtml.

Only the Cisco 3845 supports two network modules in a single chassis. This implies that this model is applicable only to large branch office design. This design has the following advantages:

- Data and voice traffic separation under normal operation
- Quick convergence in case of failure
- The distribution layer is collapsed into the edge layer, which can be scaled up
- Integrated GigabitEthernet ports freed to provide further scalability
- Compatible features with Catalyst 3750 and Catalyst 3560 family of switches and better integration with the access layer

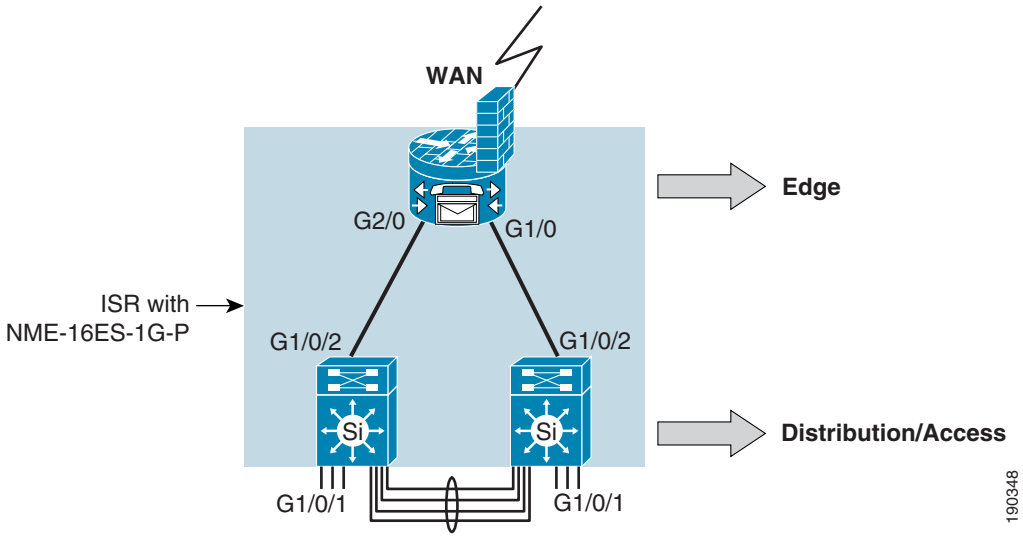
This design has the following disadvantages:

- The redundant links provide limited scalability
- The redundant topology and configuration is more complex compared to a stackable environment.
- Only the Cisco 3825 or Cisco 3845 can be used as the edge router in this design

The dual EtherSwitch Service Module design is similar to deploying two external devices connected to the ISR. However, the links between the ISR and the network modules are internal to the chassis. To configure the network modules, a session has to be established to the network services modules from the ISR. The details of the internal connectivity and the configuration to establish the session are provided in the Appendix of this guide.

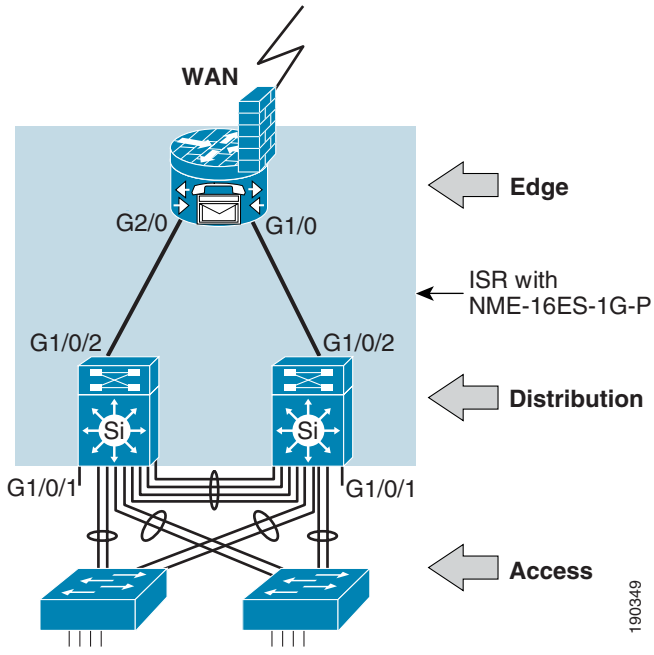
Figure 8 shows the topology using two EtherSwitch Service Modules in the ISR. The two switches are shown as external switches because they have their own CPU and communicates with the ISR and access switches through GigabitEthernet Interfaces. From a configuration perspective, the switches must be configured separately. The GigabitEthernet links between the ISR and the EtherSwitches are internal to the chassis.

Figure 8 Topology with Two Cisco EtherSwitch Service Modules in ISR



The EtherChannel between the Cisco EtherSwitch Service Modules provides the interconnectivity required for high availability. The EtherChannel has multiple members and avoids a single point of failure. Alternatively, a single Gigabit Ethernet link can be used between the switches, but is not recommended. Clients can be connected to the ports that are not used for the redundant links for high availability. For a higher fan-out, dual homed access switches must be connected, as shown in Figure 9. When these access switches are connected and the VLANs and the Rapid PVST+ are configured, the spanning tree converges, and the links go into blocking/forwarding states according to the configuration.

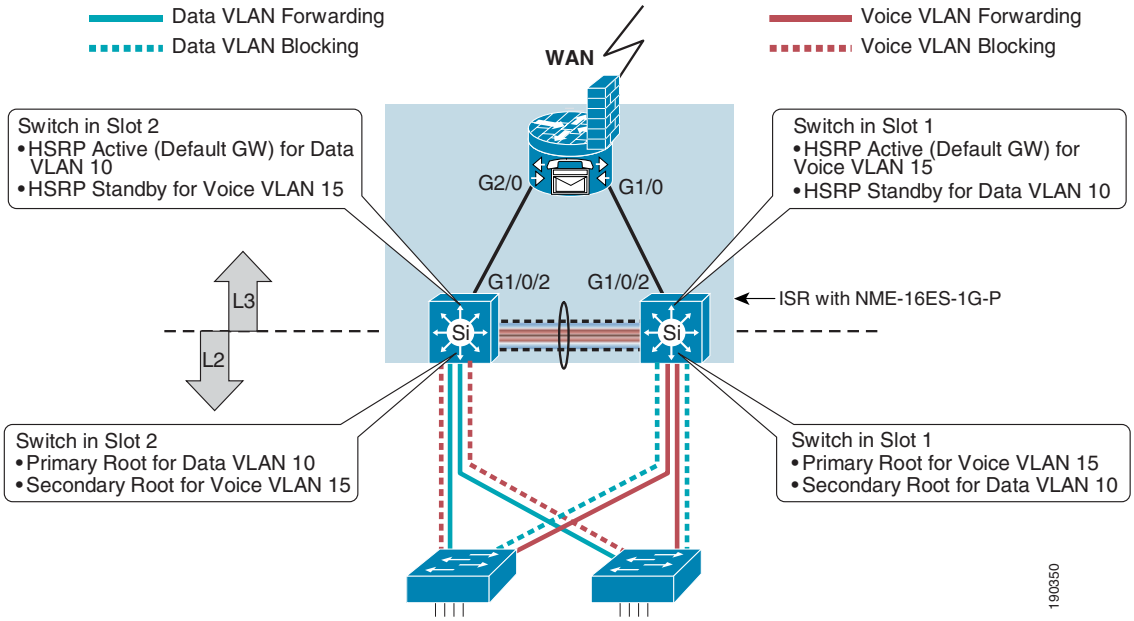
Figure 9 Topology with EtherSwitch Service Modules with a Higher Fan-out



Layer 2 Topology Details

Figure 10 provides details of the spanning tree topology with voice and data VLANs. Rapid PVST+ is used for quick convergence. The EtherSwitch Service Modules are independent of each other, and the ISR treats them as external devices from a software perspective.

Figure 10 Spanning Tree Topology with Two Single Wide EtherSwitch Modules in an ISR



At Layer 2, the EtherSwitches are configured with Rapid PVST+ for quick convergence. The primary and secondary roots of the spanning tree for different VLANs are distributed between the two switches. As shown in Figure 10, each switch is configured to be the primary root for a single service. In the topology shown, the switch in slot 2 is the primary root for data services, and switch 1 is the primary root for voice services. The link between the two switches is an EtherChannel trunk that carries all VLANs configured on the switches. EtherChannel provides the redundancy required for a highly available design. The Cisco EtherSwitch Service Modules are configured in active-active configuration for maximum utilization of switching power and bandwidth.

Note Unlike the previous designs in which there is an EtherChannel between the access and distribution without Layer 2 loops, this design has Layer 2 loops because the two switches are physically separate switches. Member ports of an EtherChannel cannot terminate on two different physical switches. Also note that only the Cisco 3845 ISR supports two EtherSwitch Service Modules. For more information, see the following URL:
http://www.cisco.com/en/US/partner/products/ps5855/products_qanda_item0900aecd8028d16a.shtml

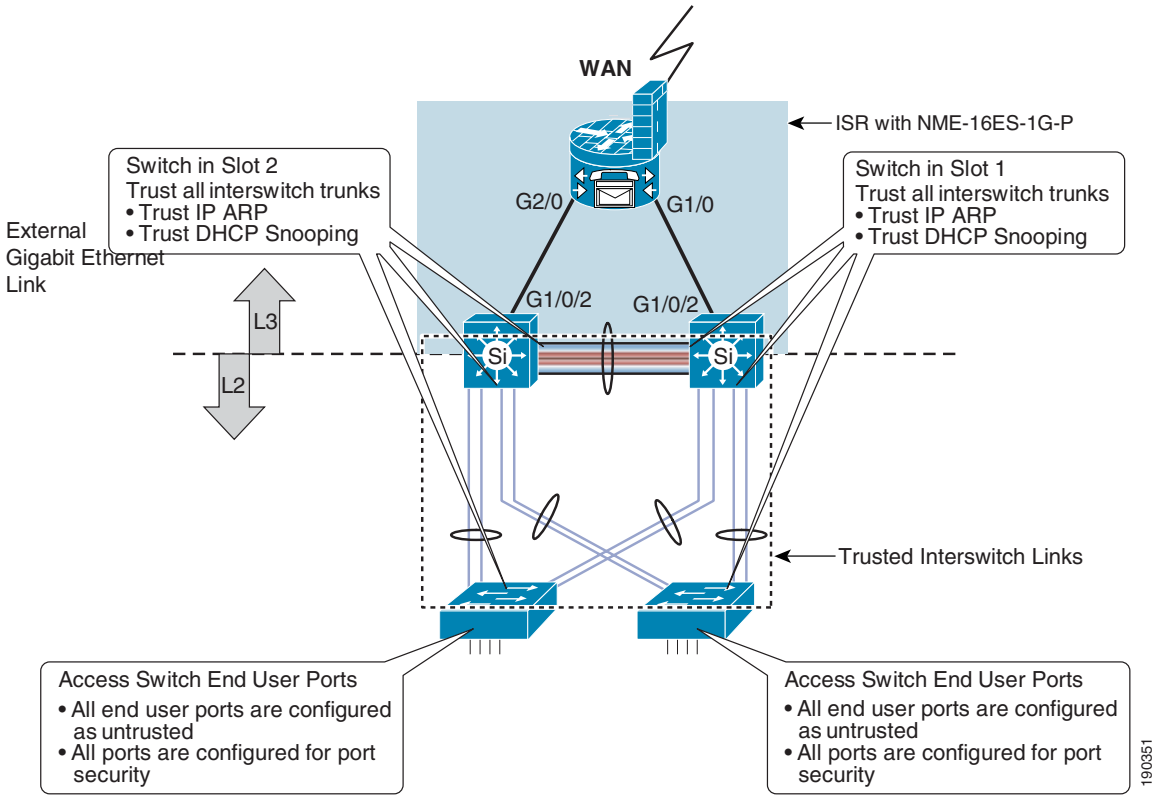
Because of the configuration of the services modules, only 10/100 ports can be used to configure an EtherChannel. Cisco recommends that the single Gigabit Ethernet interfaces of the service modules be used for advanced services rather than carrying all the VLANs between the two services modules or for scaling the network. This is done to maintain a single spanning tree topology across all access switches if access switches are used. This requirement is one of the drawbacks of this design.

Note Cisco recommends using the Gigabit Ethernet interfaces for deploying security appliance devices if required.

Layer 2 Security

As part of Layer 2 security, the inter-switch links must be configured as trusted ports. Only the ports connected to the end users are configured as untrusted ports. Figure 11 provides the details of trusted and untrusted ports. To make a port trusted, the EtherChannels must be configured as trusted ports. All ports are untrusted by default.

Figure 11 Trusted and Non-trusted Ports for Layer 2 Security



Layer 3 Topology Details

Hot Standby Routing Protocol (HSRP) on the switches provides high availability. The active HSRP IP address for a VLAN is configured on the same switch on which it is the primary root. If IP base images are used on the switches, static routes can be used to route client traffic. With voice and data VLANs as the only two VLANs, with possibly a VLAN for wireless clients and guest access, static routing should be more than sufficient. There is a single default route (gateway of last resort) configured on both the switches. This default route points to the next hop on the ISR Gigabit Ethernet interface. For example, the switch in slot 2 is the default gateway for all data traffic. The gateway of last resort on switch 2 points to the next hop IP address configured on the internal Gigabit Ethernet interface of the ISR for slot 2. If the path between the switch and the ISR breaks, the object tracking (discussed in the next section) forces the HSRP to go into standby mode for the data VLAN. This in turn forces the HSRP on the redundant

switch in slot 1 to go into active mode. The transition to standby mode forces the traffic to be bridged on the switch in slot 2 to the switch in slot 1 through the trunk between the two switches. The bridged traffic is then Layer 3 switched to the next hop IP by switch 1 in slot 1.

On the ISR, there are two routes configured for both data and voice traffic. A static route is configured dynamically based on the link between the ISR and the switches that overrides the route metrics, and forces the voice and data traffic to take different routes. This design, under normal circumstances, provides a simple way to segregate the voice and data traffic in an active-active configuration. The static route is dynamically removed under failure conditions, forcing data or voice traffic to take the alternate path.

With static routes configured on the ISR to route traffic to the end hosts or clients, the static routes have to be redistributed into the routing protocol configured.

High Availability Design for Link Failure

Typically, interfaces can be tracked if HSRP is used to guard against link failures. A unidirectional link failure might not trigger the link to go down, which causes the interface tracking to fail. This problem can occur for external as well as internal interfaces between the ISR and the Cisco EtherSwitch Service Module.

The internal GigabitEthernet links between the ISR and the Cisco EtherSwitch Service Modules provide a unique challenge for high availability when there is an internal link failure. When either the ISR or the switch links fail, the adjacent device does not detect the link failure because of the hardware architecture. Because of this caveat, tracking internal interfaces does not result in recovering from failure. Additional logic must be applied to both sides of the Gigabit Ethernet links to detect the failure. This additional logic comes from using the object tracking feature, which provides a separate tracking process that can be used to track the reachability of a host. After a success/failure event, appropriate actions can be taken. This solution can be used for both internal as well as external interfaces between the Cisco EtherSwitch Service Module and the ISR.

Note For more information on the object tracking feature, see the following URL: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a00801541be.html

In the dual EtherSwitch Service Module topology, object tracking should be deployed both at the ISR and on the Cisco EtherSwitch Service Modules. On the ISR, the reachability of the adjacent device is monitored and after success, a static route is configured to override a redundant path. ICMP echoes are used by the ISR to monitor the adjacent device. The monitoring process in Cisco IOS is called the Cisco IOS IP SLA. Cisco IOS IP SLA notifies the change in state of the monitored device to the object tracking process, and then the actions defined are taken by the object tracking process.

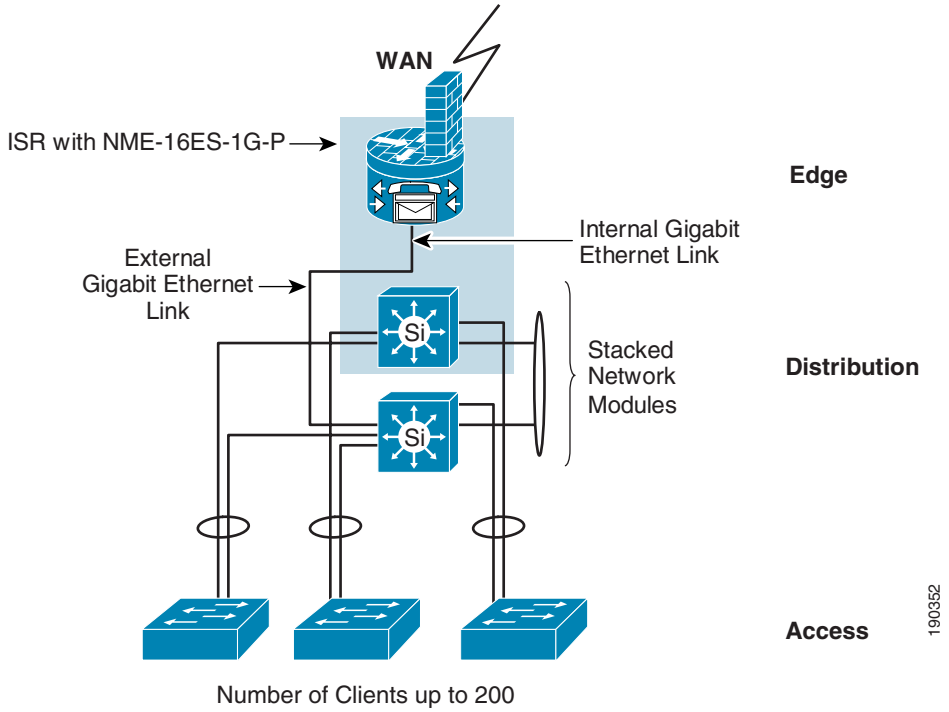
Because HSRP is used, the path is changed by changing the default gateway on the Cisco EtherSwitch Service Modules. The default gateway is changed by decrementing the priority of the active HSRP. The gateway of last resort configured on both the switches routes the packets appropriately. Because the monitoring is done on the ISR as well, appropriate action is taken to reflect the link failure.

Integrated Stackable EtherSwitch Services Module Design

From a logical point of view, there is not much difference between this design and the large office design presented in the earlier section. The physical topology is different because of the internal Gigabit Ethernet link between the ISR and the Cisco EtherSwitch Service Module. Because only a single stackable EtherSwitch Service Module is supported in an ISR chassis, an external Cisco Catalyst 3750 switch has to be used to achieve high availability and scalability.

Figure 12 shows the topology details of this design, which meets all the design goals and scales up to a large branch office design.

Figure 12 Topology using a Stackable Integrated EtherSwitch Module for the ISR



This topology is no different from a large branch office design explained in the earlier section. For details of the design, see the previous section, because there are really no differences logically. However, from a hardware point of view, there are the following two main differences:

- An external stackable switch (Cisco Catalyst 3750) must be used, along with the Cisco EtherSwitch Service Module (NME-XD-24ES-1S-P).
- Use of Object Tracking in high availability configuration is required. This feature can also be used in the earlier design.

Only one stackable EtherSwitch Service Module is supported in an ISR (for more details, see the following URL: http://www.cisco.com/en/US/partner/products/ps5855/products_qanda_item0900aecd8028d16a.shtml)

The second member of the stack must be an external Catalyst 3750 switch. This topology is similar to the large campus design discussed in the earlier section.

The second difference comes from the high availability design consideration. Because of the nature of the link status determination problem, as discussed in more detail in Section 4.1.11, object tracking and IP SLA is used to overcome the high availability problem on both sides of the link. Because of different software train releases, the commands might be different on the ISR and on the switches. However, the configurations are similar on both sides of the link.

The ease of configuration and absence of Layer 2 loops in this design is preferred to the previous design using dual Cisco EtherSwitch Service Modules. This design has a better scalability compared to the dual EtherSwitch Service Module design. The only prohibiting factor for this design is the use of a standalone switch and an EtherSwitch Service Module.

LAN Infrastructure Configuration Details

This section provides details on how to configure various features of a Branch LAN. It involves configuring the following features.

- VLAN configuration
- Voice and data VLAN
- Port security
- 802.1x for data VLAN
- QoS configuration on access ports
- EtherChannels and trunking
- Spanning tree
- Spanning tree for dual EtherSwitch Service Module topology
- HSRP configuration for dual EtherSwitch Service Module topology
- Layer 3 configuration
- Object tracking for high availability
- DHCP configuration on the default gateway
- DHCP snooping and IP Source Guard
- Dynamic ARP Inspection

Figure 13 and Figure 14 show details on where these features are configured in small, medium, and large office topologies.

Figure 13 Small and Medium Office Topology and Related Configuration

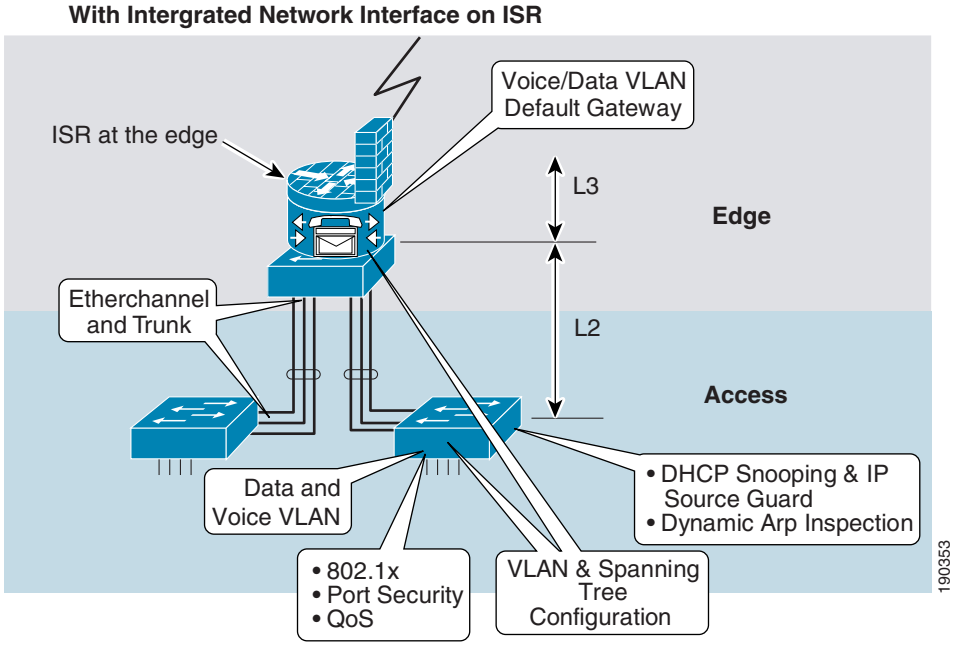
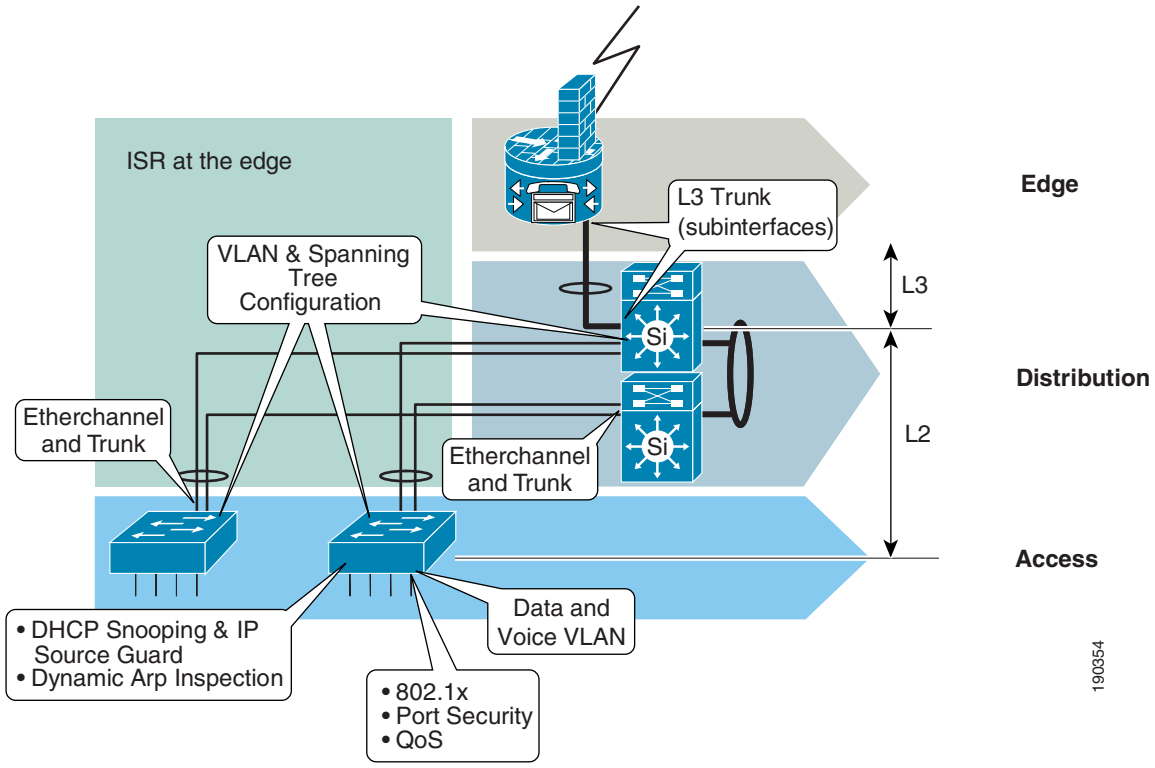


Figure 14 Large Office Topology and Related Configuration



VLAN Configuration

Before configuring VLANs, you need to define the VTP mode for the switch. There are no benefits of using VTP, so use VTP transparent mode, which also helps eliminate the VLAN misconfiguration errors being propagated. The following two devices might need the VLAN configuration in a branch topology:

- Layer 2 VLANs on the ISR
- Layer 2 VLANs on the switches

Use the following command to configure VTP mode and the VLANs on the ISR:

```
C2851#vlan database
C2851(vlan)#vtp domain Layer2Infrastructure
Changing VTP domain name from NULL to Layer2Infrastructure
C2851(vlan)#vtp transparent
Setting device to VTP TRANSPARENT mode.
```

Use the same domain name throughout the infrastructure.

On the switches connected to the ISR, use the following commands to set up the domain and VTP transparent mode:

```
c3560-1(config)#vtp domain Layer2Infrastructure
C3560-1(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
c3560-1(config)#
```

You need the following subnets and VLANs in a branch network:

- Data VLANs
- Voice VLANs
- Wireless VLANs—Typically, the wireless traffic is carried on a separate VLAN. There can be multiple VLANs associated with multiple SSIDs in the WLAN.
- Layer 3 VLANs—Each Layer 2 VLAN has to be tied to a Layer 3 VLAN interface

Use the following commands to setup the VLANs on the ISR:

```
C2851#vlan database
C2851(vlan)#
C2851(vlan)#vlan 30 state active
VLAN 70 added:
    Name: VLAN0030
    State ACTIVE
C2851(vlan)#vlan 30 name DataVLAN
VLAN 30 modified:
    Name: DataVLAN
C2851(vlan)#
```

On the switch, use the following commands to set up the VLANs:

```
c3750-1-1(config)#
c3750-1-1(config)#vlan 30
c3750-1-1(config-vlan)#name DataVLAN
c3750-1-1(config-vlan)#state active
```

Voice and Data VLAN

Voice and data VLANs are configured on the access ports to which the end users are connected. The voice and data VLANs are supported on a single interface and work with Cisco IP phones. Cisco IP phones have a switch inside that supports a 10/100 Ethernet port, which can be used as a data port. Cisco IP phones tag all packets originating from the IP phone with a voice VLAN ID. The data traffic coming from the associated Ethernet interface on the Cisco IP phone is untagged and is associated with the access VLAN on the switch port.

Voice and data VLANs can be configured using the following commands on an access switch port:

```
c2950-2#sh run int f0/1
Building configuration...

Current configuration : 167 bytes
!
interface FastEthernet0/1
 switchport access vlan 30
 switchport mode access
 switchport voice vlan 20
 spanning-tree portfast
 spanning-tree bpduguard enable
end
```

Note Cisco Discovery Protocol (CDP) must be enabled on the switch for the IP phone to work. CDP ensures that the device connected to the access port is a Cisco IP phone.

When an IP Communicator is used, the communicator operates in the data VLAN. The device (PC or laptop) does not send tagged packets to the switch. The device is associated with the data VLAN and gets a single IP address. The IP Communicator does support CDP and is able to mark the VoIP packets from a QoS perspective. The details of QoS markings are covered in the QoS section below.

Port Security

Port security is one of the modules of the Layer 2 security portfolio and is part of the access port configuration. The port security guidelines suggest that if the access port is used for both voice and data VLANs, only three MAC addresses should be allowed on the port. If the fourth MAC address shows up in the CAM tables of the switch, it is a violation of the security guidelines. The command line also provides three options if there is a security violation, as shown in the following screen:

```
c2950-2(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
```

The restrict mode is used in the following configuration, along with **port-security aging time**, as shown in the following configuration:

```
c2950-2#sh run int f0/1
Building configuration...

Current configuration : 361 bytes
!
interface FastEthernet0/1
 switchport access vlan 30
 switchport mode access
 switchport voice vlan 20
 switchport port-security
 switchport port-security maximum 3
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 spanning-tree portfast
 spanning-tree bpduguard enable
end
```

802.1x for Data VLAN

This section provides the 802.1x configuration for the switch. In addition to the switch configuration, the RADIUS server and the clients (PC/laptops) must be configured, which is not covered in this document. For more detailed information about various aspects of 802.1x, see the following URL: http://identity.cisco.com.

802.1x can be configured for both the scenarios where the PC is connected to a Cisco IP phone, and the PC is directly connected to a switch port. In either case, a VLAN can be assigned based on client credentials. A guest VLAN can also be configured on the switch port if the client does not have an 802.1x supplicant. The guest VLANs and issues related to guest VLANs are not covered in this document because of the complexity involved.

802.1x switch configuration involves the following steps:

Step 1 Configure the RADIUS server information on the switch.

```
c2950-2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
c2950-2(config)#radius-server host 20.1.2.10 auth-port 1812 acct-port 1813
c2950-2(config)#radius-server retransmit 3
c2950-2(config)#radius-server key cisco
```

The key has to match what is configured on the RADIUS server. What is shown here is an example. The key is a pre-shared secret RADIUS key used to hash and encrypt the communication between the switch and the RADIUS server.

Step 2 Configure support to send the request to the RADIUS server:

```
c2950-2(config)#aaa new-model
c2950-2(config)#aaa authentication dot1x default group radius
c2950-2(config)#aaa authorization network default group radius
c2950-2(config)#dot1x system-auth-control
```

The command **aaa authorization network default group radius** ensures that the VLANs can be pushed from the RADIUS server to the switch after successful authentication of the clients so that the clients are placed in the VLANs provided by the RADIUS server.

Step 3 Finally, configure the access ports on the access switches to support 802.1x. The configuration below is for a switch port that supports an IP Phone + PC. The 802.1x related commands are shown in red. Note that the access VLAN is not specified in the following configuration. The VLAN is assigned by the RADIUS server based on the client credentials.

```
c2950-2#sh run int f0/2
Building configuration...

Current configuration : 521 bytes
!
interface FastEthernet0/2
 switchport mode access
 switchport voice vlan 20
 switchport port-security
 switchport port-security maximum 3
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 dot1x port-control auto
 dot1x host-mode multi-host
 macro description cisco-phone
 spanning-tree portfast
 spanning-tree bpduguard enable
end
```

For a scenario where the VLAN is not dynamically assigned by the RADIUS server, specify the VLAN as shown in the following configuration:

```
c2950-1(config-if)#switchport access vlan 30
```

For the scenario where the user connects directly to the switch port, the configuration is as shown below:

```
c2950-2(config)#switchport mode access
c2950-2(config)#switchport access vlan 30
c2950-2(config)#dot1x port-control auto
c2950-1(config-if)#dot1x host-mode single-host
```

Note that the access VLAN is configured in the above configuration. If VLANs should be assigned by the RADIUS server, use the following configuration:

```
c2950-2(config)#switchport mode access
c2950-2(config)#dot1x port-control auto
```

QoS Configuration on Access Ports

The trust boundaries established as described in the sections above dictate the QoS configuration on the access ports. If the end device is trusted, the CoS and DSCP values can be allowed on the access switches. If the end device is not trusted, the access switch provides the capability to remark traffic. More detailed information about the various trust models and QoS configuration can be found in the Cisco Press publication mentioned in the Reference section, which provides a more comprehensive description of the various models and switch capabilities that can be used. This document focuses on a baseline architecture, and only relevant configurations are shown here. In this section, only the partially trusted model (Cisco IP phone + PC) and untrusted models are provided for various access switches.

CDP, which is the Cisco proprietary protocol to determine the neighbor, is used on the switches to determine the trustworthiness of the devices attached to the switches. After the trustworthiness is determined, the trust can be extended to the trusted device. The Cisco IP phone falls under the partially trusted model because a PC can be attached to the Cisco IP phone and the traffic from the PC is not trusted. All the traffic from the Cisco IP phone that is tagged with the voice VLAN is trusted.

All the Cisco IP phones have the ability to mark 802.1Q/p CoS values for both the control and voice packets. Some models of Cisco IP phones may not have the additional Ethernet port to support the PC. Policing on the switch ports can be used to ensure that proper bandwidth is allocated for legitimate applications. The tighter or more granular policers achieve the end goal of policing unwanted traffic and reserving the bandwidth for legitimate applications. For details of algorithms used for policing, see the Cisco Press Book in the reference section.

Note Not all switches provide the same level of granularity when it comes to policing. Based on the policing and QoS requirements, different access switches might have to be deployed. See the product literature for more information on what is supported on the platforms.

Cisco Catalyst 2950 Partially Trusted Model

The following configuration snippet provides the global configuration required for Cisco Catalyst 2950 switches. The relevant configuration is shown in red.

```
c2950-1#sh run
Building configuration...

Current configuration : 8723 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c2950-1
!
!
wrr-queue bandwidth 5 25 70 0
wrr-queue cos-map 1 1
wrr-queue cos-map 2 0
wrr-queue cos-map 3 2 3 4 6 7
wrr-queue cos-map 4 5
!
class-map match-all DVLAN-ANY
  match access-group name DVLAN-ANY
class-map match-all VVLAN-ANY
```

```
  match access-group name VVLAN-ANY
!
!
policy-map IPPHONE+PC
  class VVLAN-ANY
    police 1000000 8192 exceed-action drop
  class DVLAN-ANY
    set ip dscp 0
    police 5000000 8192 exceed-action dscp 8
!
mls qos map cos-dscp 0 8 16 24 32 46 48 56
```

The configuration specifies that if the rate is less than 1 Mbps, the voice VLAN should let the traffic through; and if the traffic rate is less than 5 Mbps, the data VLAN should let the traffic through. Otherwise, the traffic is discarded.

Define the access lists for both voice and data VLAN as follows:

```
c2950-1#sh access-lists
Standard IP access list DVLAN-ANY
    permit 10.1.30.0, wildcard bits 0.0.0.255
Standard IP access list VVLAN-ANY
    permit 10.1.20.0, wildcard bits 0.0.0.255
c2950-1#
```

For the policing to take effect, apply the QoS policy to specific interfaces as follows:

```
c2950-1#sh run int f0/1
Building configuration...

Current configuration : 451 bytes
!
interface FastEthernet0/1
 switchport access vlan 30
 switchport mode access
 switchport voice vlan 20
 switchport port-security
 switchport port-security maximum 3
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 service-policy input IPPHONE+PC
 mls qos trust device cisco-phone
 mls qos trust cos
 spanning-tree portfast
 spanning-tree bpduguard enable
end
```

The Catalyst 2950 can be configured in 4Q1T mode or 1P3Q1T mode. The latter is recommended. The following commands are used to configure queuing:

```
c2950-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
c2950-1(config)#wrr-queue bandwidth 5 25 70 0
c2950-1(config)#wrr-queue cos-map 1 1
c2950-1(config)#wrr-queue cos-map 2 0
c2950-1(config)#wrr-queue cos-map 3 2 3 4 5 7
c2950-1(config)#wrr-queue cos-map 4 5
c2950-1(config)#end
c2950-1#
```

Cisco Catalyst 3550 Partially Trusted Model

The QoS support in the Cisco Catalyst 3550 is far superior to the Catalyst 2950, and can become very complex. Only the baseline configurations for voice and data in a partially trusted model and untrusted model are provided in this document. For advanced QoS configuration and recent enhancements to QoS, see the Cisco Press publication and current software configuration guide.

Note End Of Sale (EOS) has been announced for the Cisco Catalyst 3550 switch. The following configuration is only for the sake of completeness and should not be construed as a recommended switch.

Step 1 If QoS is disabled, enable it as follows:

```
3550#sh mls qos
QoS is disabled

3550#conf t
Enter configuration commands, one per line. End with CNTL/Z.
3550(config)#mls qos
QoS: ensure flow-control on all interfaces are OFF for proper operation.
3550(config)#exit
3550#sh mls qos
8w2d: %SYS-5-CONFIG_I: Configured from console by console
QoS is enabled
```

As the message suggests, the flow control has to be turned off for proper operation of QoS on all interfaces.

Step 2 Map CoS 5 to DSCP EF and mark the excess data and voice VLAN traffic to scavenger (CS1) using the following commands:

```
3550(config)#mls qos map cos-dscp 0 8 16 24 32 46 48 56
3550(config)#mls qos map policed-dscp 0 24 to 8
```

Step 3 Configure the class maps with match policies for voice and call signaling as follows. Note that 26 and 24 represent the old call signaling and new call signaling values.

```
3550(config)#class-map match-all VOICE
3550(config-cmap)#match ip dscp 46
3550(config-cmap)#class-map match-any CALL-SIGNALING
3550(config-cmap)#match ip dscp 26
3550(config-cmap)#match ip dscp 24
```

Step 4 Configure the class map to identify voice VLAN and packets with DSCP set to EF, as follows:

```
3550(config-cmap)#class-map match-all VVLAN-VOICE
3550(config-cmap)#match vlan 20
3550(config-cmap)#match class-map VOICE
```

Step 5 The following configuration identifies call signaling traffic with DSCP AF31 and CS3:

```
3550(config)#class-map match-all VVLAN-CALL-SIGNALING
3550(config-cmap)#match vlan 20
3550(config-cmap)#match class-map CALL-SIGNALING
3550(config-cmap)#
```

Step 6 Identify any other traffic in voice VLAN with the following configuration:

```
3550(config)#class-map match-all ANY
3550(config-cmap)#match access-group name ANY
3550(config-cmap)#exit
3550(config)#class-map match-all VVLAN-ANY
```

```
3550(config-cmap)#match vlan 20
3550(config-cmap)#match class-map ANY
```

Step 7 A similar configuration for data VLAN follows. However, there is no signaling traffic on data VLAN.

```
3550(config)#class-map match-all DVLAN-ANY
3550(config-cmap)#match vlan 30
3550(config-cmap)#match class-map ANY
```

Step 8 Configure the IP phone + PC model policy to set different DSCP values on voice and data traffic, and to police voice and data traffic with the following commands. Note that there is an advanced model that classifies different traffic patterns within the data and voice VLANs and polices different traffic patterns, which is not discussed in this document.

```
3550(config)#policy-map IPPHONE+PC
3550(config-pmap)#class VVLAN-VOICE
3550(config-pmap-c)#set ip dscp 46
3550(config-pmap-c)#police 128000 8000 exceed-action drop
3550(config-pmap-c)#class VVLAN-CALL-SIGNALING
3550(config-pmap-c)#set ip dscp 24
3550(config-pmap-c)#police 32000 8000 exceed-action policed-dscp-transmit
3550(config-pmap-c)#class VVLAN-ANY
3550(config-pmap-c)#set ip dscp 0
3550(config-pmap-c)#police 32000 8000 exceed-action policed-dscp-transmit
3550(config-pmap-c)#class DVLAN-ANY
3550(config-pmap-c)#set ip dscp 0
3550(config-pmap-c)#police 5000000 8000 exceed-action policed-dscp-transmit
3550(config-pmap-c)#exit
3550(config-pmap)#exit
3550(config)#
```

The above configuration polices signaling traffic, and traffic exceeding 32 Kbps is discarded. For the data VLAN, the allowed bit rate is 5 Mbps.

Step 9 Apply the service policy on the interfaces as follows:

```
3550(config)#int f0/14
3550(config-if)#sw
3550(config-if)#mls qos trust device cisco-phone
3550(config-if)#service-policy input IPPHONE+PC
```

Step 10 For the configuration to be complete, define the access list that was used to identify all other traffic on voice and data VLANs, as follows:

```
3550(config)#ip access-list standard ANY
3550(config-std-nacl)#permit any
3550(config-std-nacl)#end
3550#
```

The Cisco Catalyst 3550 supports a 1P3Q1T queuing model. Unlike the Catalyst 2950, the queuing parameters are set on a per-interface basis.

Step 11 Use the following command to set the queuing parameters for the four different queues:

```
3550(config)#interface range f0/1 - 20
3550(config-if-range)#wrr-queue bandwidth 5 25 70 1
3550(config-if-range)#wrr-queue cos-map 1 1
3550(config-if-range)#wrr-queue cos-map 2 0
3550(config-if-range)#wrr-queue cos-map 3 2 3 4 6 7
3550(config-if-range)#wrr-queue cos-map 4 5
3550(config-if-range)#priority-queue out
3550(config-if-range)#
```

Catalyst 2970/3560/3750 Partially Trusted Model

The latest version of the software supports per-VLAN QoS. It is possible that per-VLAN QoS provides some advantages over the configuration provided. However, because of time constraints, the configurations are not provided in this version of the document. In the following configuration below, access lists are used to match the voice and signaling traffic. The configuration for the Cisco Catalyst 2970, 3560 and 3750 is similar. An example of the configuration follows.

Step 1 The following configuration modifies CoS-to-DSCP mapping from CoS 5 to DSCP EF:

```
c3750-1-1(config)#mls qos map cos-dscp 0 8 16 24 32 46 48 56
```

Step 2 The following configuration marks excess voice and data traffic as scavenger traffic:

```
c3750-1-1(config)#mls qos map policed-dscp 0 24 to 8
```

Step 3 Configure class maps for voice, signaling, and any VLAN as follows:

```
c3750-1-1(config)# class-map match-all VVLAN-VOICE
c3750-1-1(config-cmap)#match access-group name VVLAN-VOICE
c3750-1-1(config-cmap)#class-map match-all VVLAN-CALL-SIGNALLING
c3750-1-1(config-cmap)#match access-group name VVLAN-CALL-SIGNALLING
c3750-1-1(config-cmap)#
c3750-1-1(config-cmap)#class-map match-all VVLAN-ANY
c3750-1-1(config-cmap)#match access-group name VVLAN-ANY
c3750-1-1(config-cmap)#
```

Step 4 Configure policy maps for the IPPHONE+PC basic model as follows:

```
c3750-1-1(config-cmap)#policy-map IPPHONE+PC-BASIC
c3750-1-1(config-pmap)#class VVLAN-VOICE
c3750-1-1(config-pmap-c)#set ip dscp 46
c3750-1-1(config-pmap-c)#police 128000 8000 exceed-action drop
c3750-1-1(config-pmap-c)#
```

Step 5 Police voice signaling traffic and mark down out-of-profile traffic as scavenger traffic, as follows:

```
c3750-1-1(config-pmap-c)#class VVLAN-CALL-SIGNALLING
c3750-1-1(config-pmap-c)#set ip dscp 24
c3750-1-1(config-pmap-c)#police 32000 8000 exceed-action policed-dscp-transmit
```

Step 6 Repeat the configuration to mark down out-of-profile traffic as scavenger traffic, as follows:

```
c3750-1-1(config-pmap-c)#class VVLAN-ANY
c3750-1-1(config-pmap-c)#set ip dscp 0
c3750-1-1(config-pmap-c)#police 32000 8000 exceed-action policed-dscp-transmit
c3750-1-1(config-pmap-c)#class class-default
c3750-1-1(config-pmap-c)#set ip dscp 0
c3750-1-1(config-pmap-c)#police 5000000 8000 exceed-action policed-dscp-transmit
c3750-1-1(config-pmap-c)#exit
c3750-1-1(config-pmap)#exit
```

Step 7 Apply the QoS configuration to the interfaces. It is assumed that the access and voice VLANs are already configured.

```
c3750-1-1(config)#int f0/2
c3750-1-1(config-if)#mls qos trust device cisco-phone
c3750-1-1(config-if)#service-policy input IPPHONE+PC-BASIC
c3750-1-1(config-if)#exit
c3750-1-1(config)#
```

Step 8 Define the IP access lists to match voice and data traffic, as follows:

```
c3750-1-1(config)#ip access-list extended VVLAN-VOICE
```

```
c3750-1-1(config-ext-nacl)#permit udp 10.1.20.0 0.0.0.255 any range 16384 32767
dscp ef
c3750-1-1(config-ext-nacl)#exit
c3750-1-1(config)#
c3750-1-1(config)#
c3750-1-1(config)#ip access-list extended VVLAN-CALL-SIGNALLING
c3750-1-1(config-ext-nacl)#permit tcp 10.1.20.0 0.0.0.255 any range 2000 2002 dscp
af31
c3750-1-1(config-ext-nacl)#permit tcp 10.1.20.0 0.0.0.255 any range 2000 2002 dscp
cs3
c3750-1-1(config-ext-nacl)#exit

c3750-1-1(config)#ip access-list extended VVLAN-ANY
c3750-1-1(config-ext-nacl)#permit ip 10.1.20.0 0.0.0.255 any
c3750-1-1(config-ext-nacl)#end
c3750-1-1#
```

EtherChannel and Trunking

EtherChannel provides the required link redundancy between switches in addition to load balancing based on the source or destination MAC addresses. If a stackable switch is involved in an EtherChannel between two switches, choose the member ports to be on different switches across the stack. Use the following steps to configure EtherChannels and trunking between two switches in the topology. The following steps are to be used to set up EtherChannel and then Layer 2 trunks and encapsulation:

- Configure each member interface to be part of the EtherChannel.
- Configure the ports to be in trunk mode
- Configure the ports to use dot1q encapsulation on the trunk

The following configuration shows the relevant configuration:

```
interface FastEthernet1/0/1
 switchport trunk encapsulation dot1q! Configure the encapsulation to be used on the trunk
 switchport mode trunk    ! Trunk Configuration
 channel-group 2 mode on  ! EtherChannel Configuration
!
.
.
interface FastEthernet2/0/1
 switchport trunk encapsulation dot1q! Configure the encapsulation to be used on the trunk
 switchport mode trunk    ! Trunk Configuration
 channel-group 1 mode on  ! EtherChannel Configuration
!
```

Note On some switches, the encapsulation command does not appear, which simply means that only dot1q encapsulation is supported for the trunk interface.

The following configuration appears on the switch when the EtherChannel, trunk, and encapsulation are configured:

```
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

After the trunk is configured, allow only those VLANs that need to be carried on the trunk. In addition to configuring specific VLANs that need to be allowed, configure the native VLAN on the trunk. Use any VLAN other than VLAN 1 as the native VLAN.

Note Although Cisco recommends allowing those VLANs that are of interest on the trunks, the 16-port and double-wide Ethernet switch for the ISRs requires certain VLANs to be allowed on the trunked interface.

The following configuration shows how to configure allowed VLANs on the trunk:

```
c3750-1(config)#int po1
c3750-1(config-if)#switchport trunk allowed vlan 20,30,40,50,60
```

Later, if changes need to be made, the VLANs can be added or removed using the appropriate keywords, as shown in the following screen:

```
c3750-1(config)#int po1
c3750-1(config-if)#switchport trunk allowed vlan ?
  WORD    VLAN IDs of the allowed VLANs when this port is in trunking mode
  add       add VLANs to the current list
  all       all VLANs
  except    all VLANs except the following
  none      no VLANs
  remove    remove VLANs from the current list
```

On the ISR, if no switching is used (small office design), or to connect the ISR and the distribution switch, use the following commands to configure the Layer 3 trunk. Configure a sub-interface for each VLAN configured or used in the topology.

```
interface GigabitEthernet0/1.50
 encapsulation dot1Q 50 native
 ip address 10.1.50.1 255.255.255.0
!
```

Layer 3 trunking is provided on sub-interfaces. However, on the switch side, if a distribution switch is involved (large office design), use SVIs instead of sub-interfaces.

Spanning Tree

Spanning tree is configured on switches. If a distribution switch is used (large office topology), spanning tree configurations are limited to the access switch and the distribution switch. In a small office and medium office design, if a switch is used on the ISR, spanning tree is configured both on the ISR and the access switches. The main difference from a spanning tree perspective between the large office design and the small/medium office design is the spanning tree mode used. In the case of a large office design, the spanning tree mode used on both the distribution and the access layer is the same. In the case of a small/medium office design, the spanning tree mode on the ISR is 802.1D for each instance of the VLAN, and the spanning tree mode on the access switch will be either Rapid PVST+ or MST. Cisco recommends using Rapid PVST+ when available. Rapid PVST+ interoperates with 802.1D spanning tree.

Spanning tree configuration involves the following:

- Mode of spanning tree used
- Root bridge configuration
- Spanning tree protection features such as BPDU Guard, Loop Guard, and UniDirectional Link Detection (UDLD)

To configure Rapid PVST+, enter the following global command on a switch:

```
c3560-2(config)#spanning-tree mode rapid-pvst
```

The next step is to assign the primary root switch. To configure the primary root, enter the following command:

```
c3750-1(config)#spanning-tree vlan 20,30,40,50,60 root primary
```

Typically, in a Layer 2 network, there is a redundant device that assumes the root responsibilities if the primary root device fails. This redundant device is called the secondary root. However, in the proposed topology, the redundant device is either embedded in a stack (distribution switch and large office design), or there is no redundant switch (small/medium office design). This eliminates the need to configure a secondary root. In the case of a small/medium office design involving a switch in the ISR, if the device fails, there is no connectivity, which brings down the network. In the case of a large office design, if one of the devices in the stack fails, the connectivity is maintained because of the built-in redundancy of the stack.

Note With Rapid PVST+, there is no need for UplinkFast and BackboneFast. Configuring Rapid PVST+ on all the devices to belong to the same VTP domain ensures that these features are enabled.

On the distribution switch and access switch, configuring the following command is recommended to protect against EtherChannel misconfiguration:

```
c3750-1(config)#spanning-tree etherchannel guard misconfig
```

With the MAC address reduction, the above commands assign priorities as follows:

- Root bridge priority—24576 (instead of 8192 without MAC address reduction)
- Regular bridge priority—32768

To protect from inadvertent loops, it is possible to enable a feature called Loop Guard on the access and distribution switches to protect from loops. This is a global command and can be configured as follows:

```
c2950-1(config)#spanning-tree loopguard default
```

This will enable Loop Guard on all the ports. Cisco recommends that Loop Guard be enabled on both root and non-root switches.

Another feature that can be used to prevent loops because of hardware problems is UDLD. With RSTP, UDLD can still be used to prevent loops. UDLD cannot detect loops that occur after the topology has already converged. A link that suddenly becomes unidirectional causes the spanning tree topology to converge within 7 seconds. It takes 6 seconds to detect missing Bridge Protocol Data Units (BPDUs), and 1 second to send the proposal and receive an agreement. UDLD can detect a unidirectional link in 21 seconds with a message interval of 7 seconds, which is more than the time it takes for spanning tree to converge.

Loop Guard and UDLD complement each other, and therefore UDLD should also be enabled globally. To enable these features, enter the following commands:

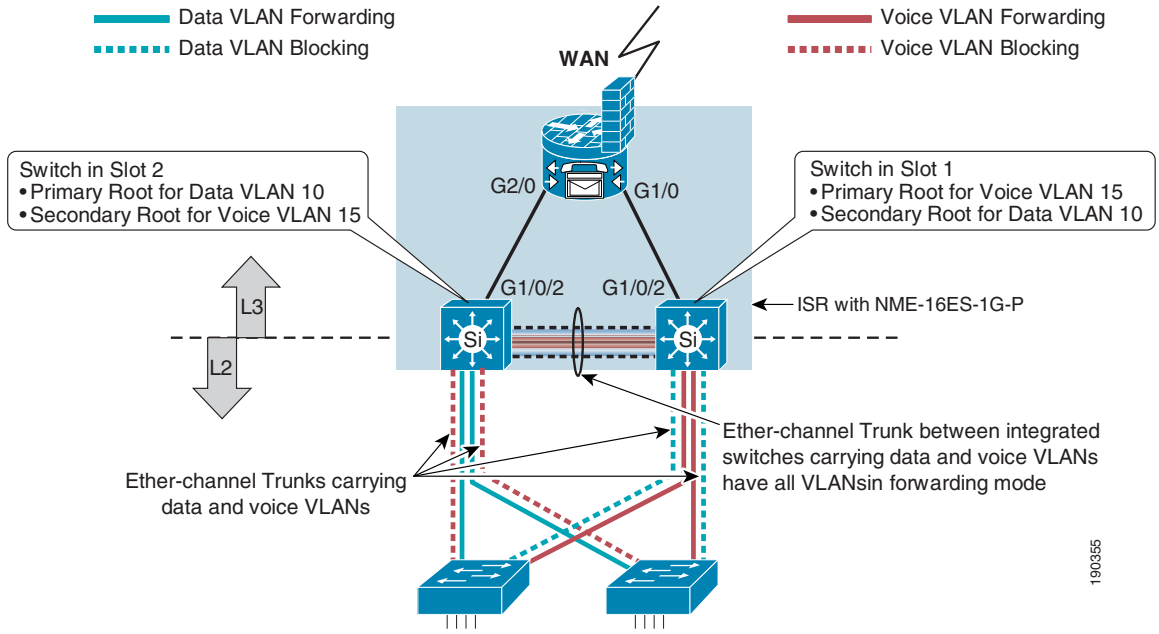
```
c2950-1(config)#udld enable
c2950-1(config)#udld message time 7
```

Note The Root Guard feature is not available. With future Ethernet switch cards, it will be available and provides a more robust Layer 2 design when used on the root bridges.

Spanning Tree for Dual EtherSwitch Services Module Topology

Spanning tree configuration for dual EtherSwitch Service Module topology is different as compared to the topology where there are no Layer 2 loops. This topology also provides load sharing in an active-active configuration, and also provides high availability in case of switch or link failure. Figure 15 shows the Layer 2 topology of the multilayer switch. The switches are configured to be in active-active mode. Figure 15 shows the details of how the switches are configured and the forwarding and blocking links as a result.

Figure 15 Layer 2 Topology of Integrated Multilayer Switches and Access Switches



On the switch in slot 1, perform the following steps.

Step 1 Enable Rapid PVST +

Step 2 Configure the primary and secondary root as follows:

```
NME16Slot1(config)#spanning-tree mode rapid-pvst
NME16Slot1(config)#spanning-tree extend system-id
NME16Slot1(config)#spanning-tree vlan 15 root primary
NME16Slot1(config)#spanning-tree vlan 10 root secondary
```

Step 3 Tag all VLANs including the native VLAN. This ensures that all traffic is tagged on inter-switch links.

```
NME16Slot1(config)#vlan dot1q tag native
```

Step 4 Enable Loop Guard as follows:

```
NME16Slot1(config)#spanning-tree loopguard default
```

Step 5 Enable EtherChannel misconfiguration guard as follows:

```
NME16Slot1(config)#spanning-tree etherchannel guard misconfig
```

On the switch in slot 2, perform the following steps:

Step 1 Enable Rapid PVST +

Step 2 Configure primary and secondary root as follows:

```
NME16Slot2(config)#spanning-tree mode rapid-pvst
NME16Slot2(config)#spanning-tree extend system-id
NME16Slot2(config)#spanning-tree vlan 10 root primary
NME16Slot2(config)#spanning-tree vlan 15 root secondary
```

Step 3 Tag all VLANs including the native VLAN. This ensures all traffic is tagged on inter-switch links.

```
NME16Slot2(config)#vlan dot1q tag native
```

Step 4 Enable Loop Guard as follows:

```
NME16Slot2(config)#spanning-tree loopguard default
```

Step 5 Enable EtherChannel misconfiguration guard as follows:

```
NME16Slot2(config)#spanning-tree etherchannel guard misconfig
```

The following configurations are done on all the access switches using the commands shown above. On the access switches, perform the following steps:

1. Configure Rapid PVST+.
2. Enable tagging for all VLANs including native VLAN.
3. Enable Loop Guard.

HSRP Configuration for Dual EtherSwitch Services Module Topology

HSRP Configuration for Switch 1 Voice VLAN

- Poll timers and hold timers—Set the poll timers and the hold timers in msecs for quick transition (highlighted in turquoise)
- Priority—Ensure that the standby priority of the Active HSRP is higher. This switch is in standby mode under normal conditions. So the default priority (100) is used.
- Preemption—Preemption allows the switch to transition to HSRP active state under failure conditions of the second switch. Configure preemption for the voice VLAN (highlighted in green).
- Tracking—Tracking is configured (highlighted in gray). The tracked object is the IP address on the other side of the internal link between the switch and the ISR. Because tracking the link does not work, host tracking has to be enabled to ensure the link condition. The configuration decrements the priority by 20 indicating to the HSRP peer that the internal link between the switch and the ISR went down. This triggers HSRP transition.

Note See the configuration in Object Tracking for High Availability, page 39 to complete the tracking configuration.

```
NME16Slot1#sh run int vlan 10
Building configuration...
```

```
Current configuration : 246 bytes
!
interface Vlan10
 description VoiceVLAN10
 ip address 10.1.10.3 255.255.255.0
 no ip redirects
 no ip proxy-arp
 standby 1 ip 10.1.10.1
 standby 1 timers msec 100 msec 400
 standby 1 preempt delay reload 60
 standby 1 track 1 decrement 20
end
```

HSRP Configuration for Switch 1 Data VLAN

- Poll timers and hold timers—Set the poll timers and the hold timers in seconds (highlighted in turquoise). Because the data applications are resilient to packet drops, setting a poll timer of 1 second and hold timer of 4 seconds allows quick failover and recovery.
- Priority—For the voice VLAN, the priority is 110. For the data VLAN, the default priority (100) is used. Note that the data VLAN is secondary root on this switch.
- Preemption—For quick preemption use minimum delay of 0 seconds and 60 seconds for reload (highlighted in yellow). The reload delay allows time to stabilize after a reload before transitioning into active state.

```
NME16Slot1(config-if)#standby 1 preempt delay minimum 0 reload 60
```

- Tracking—Tracking is configured (highlighted in gray). The tracked object is the IP address on the other side of the internal link between the switch and the ISR. Because tracking the link does not work, host tracking has to be enabled to ensure the link condition. The configuration decrements the priority by 20, indicating to the HSRP peer that the internal link between the switch and the ISR went down. This triggers HSRP transition.

```
NME16Slot1#sh run int vlan 15
Building configuration...

Current configuration : 267 bytes
!
interface Vlan15
 description DataVLAN
 ip address 10.1.15.3 255.255.255.0
 no ip redirects
 no ip proxy-arp
 standby 1 ip 10.1.15.1
 standby 1 timers 1 4
 standby 1 priority 110
 standby 1 preempt delay reload 60
 standby 1 track 1 decrement 20
end
```

HSRP Configuration for Switch 2 Voice VLAN

The configuration on switch 2 is reversed for voice and data VLANs when compared with the configurations on voice and data VLANs for switch 1.

```
NME16Slot2#sh run int vlan10
Building configuration...
```

```
Current configuration : 268 bytes
!
interface Vlan10
 description VoiceVLAN
 ip address 10.1.10.2 255.255.255.0
 no ip redirects
 no ip proxy-arp
 standby 1 ip 10.1.10.1
 standby 1 timers msec 100 msec 400
 standby 1 priority 110
 standby 1 preempt delay reload 60
 standby 1 track 1 decrement 20
end
```

HSRP Configuration for Switch 2 Data VLAN

```
NME16Slot2#sh run int vlan15
Building configuration...

Current configuration : 232 bytes
!
interface Vlan15
 description VoiceVLAN15
 ip address 10.1.15.2 255.255.255.0
 no ip redirects
 no ip proxy-arp
 standby 1 ip 10.1.15.1
 standby 1 timers 1 4
 standby 1 preempt delay reload 60
 standby 1 track 1 decrement 20
end
```

Layer 3 Configuration

Layer 3 handoff typically happens either at the distribution or the edge layer, depending on which architecture is chosen. The Layer 3 handoff is done by configuring the default gateway either on the distribution or the edge layer. Some cases might require that the default gateway be configured on the ISR at the edge layer. In such cases, the Layer 2 VLAN has to be carried all the way to the ISR. Again, do not do this unless it is absolutely necessary.

Layer 3 configuration is relatively straightforward and follows the standard procedure of defining an IP address either on the SVI (if EtherSwitch is used), or on the sub-interface if integrated interfaces are used. If integrated interfaces are used, make sure to configure the data VLAN interface as the native VLAN on the sub-interface.

Step 1 Configure a sub-interface on the integrated interfaces of the ISR as follows:

```
C2851(config)#int g0/0.11
C2851(config-subif)# encapsulation dot1Q 20 native
C2851(config-subif)#ip address 10.1.20.1 255.255.255.0
C2851(config-subif)#exit
```

Step 2 Configure an SVI for an ISR with an EtherSwitch in it as follows:

```
C2851(config)#int vlan 30
C2851(config-if)#ip address 10.1.30.1 255.255.255.0
C2851(config-if)#exit
C2851(config)#
```

The Layer 2 configuration is provided in previous sections.

Step 3 Enable EIGRP and provide all the network information and redistribute the static routes if required. Only the basic configuration is provided here. Also note that only the LAN networks are shown. The WAN part of the configuration is not provided in this document.

```
C2851#show run | begin router eigrp
router eigrp 1
 network 10.1.20.0 0.0.0.255
 network 10.1.30.0 0.0.0.255
 auto-summary
!
```

If static routes are configured on the ISR, they can be redistributed into EIGRP. (See the Cisco IOS configuration guide for various ways of redistributing the routes.) For both SVIs and integrated interfaces with dot1q encapsulation facing the distribution switch or access switch, the route updates can be suppressed on those interfaces to reduce the unnecessary traffic on VLANs at the access switches. Use the command **passive-interface** <*sub-interface or vlan interface*> under **router eigrp** <*process*>.

For a large office design, there are two options. The first option is to enable dynamic routing on the distribution switch and to advertise all networks. This is really straightforward. The type of WAN link dictates how the route optimization needs to be done. Concerning the distribution layer, there is not much impact with the number of routes. The second option is to use static routing on the distribution switch. The static routes on the distribution are typically a default route to the edge router. Configure static routes on the edge router for inbound traffic and advertise the static routes to the remote router. With this option, static routes have to be configured on the edge router and advertised for the LANs incoming traffic.

The dynamic routing configurations are as follows:

```
c3750-1#sh run | begin router eigrp
router eigrp 1
 network 10.1.10.0 0.0.0.255
 network 10.1.11.0 0.0.0.255
 network 10.1.20.0 0.0.0.255
 network 10.1.30.0 0.0.0.255
 network 10.1.40.0 0.0.0.255
 network 10.1.70.0 0.0.0.255
 auto-summary
!

C2851#sh run | begin router eigrp 1
router eigrp 1
 network 1.1.1.0 0.0.0.255
 network 2.2.2.2 0.0.0.0
 network 10.1.10.0 0.0.0.255
 auto-summary
!
```

Object Tracking for High Availability

Object tracking is configured on both the switches and the ISR to overcome the hardware architecture limitation. To ensure the link up condition, the IP addresses on either side of the link has to be probed using ICMP Echoes. So the ISR and both the switches have to send probes to determine the link condition.

Note For more information on object tracking, see the following URL: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a00801541be.html#wp1090394

Object Tracking on ISR

Under normal circumstances (if probes are successful), the ISR installs a static route to override the static route with a lower metric pointing to the alternate path. If the probes fail, the ISR automatically removes the static route corresponding to that path; thus, the alternate path is used to route the traffic.

Two IP SLA monitoring events must be set up (one for each internal interface), as follows (highlighted with different colors):

```
c3845#sh run | begin ip sla monitor
ip sla monitor 1
 type echo protocol ipIcmpEcho 10.1.2.2 source-ipaddr 10.1.2.1
 timeout 400
ip sla monitor schedule 1 life forever start-time now
ip sla monitor 2
 type echo protocol ipIcmpEcho 10.1.1.2 source-ipaddr 10.1.1.1
 timeout 400
ip sla monitor schedule 2 life forever start-time now
!
c3845#sh run | begin track
track 1 rtr 1 reachability
 delay up 60
!
track 2 rtr 2 reachability
 delay up 60
!
```

Conditional Static Routes on ISR

Two conditional static routes must be configured to route the traffic. These routes are as follows (highlighted yellow). These conditional static routes override the alternate static routes shown (highlighted in green). Under failure conditions, depending on the failure, a specific conditional static route is removed by the tracking process installing the alternate route in the routing table.

```
c3845#sh run | begin ip route
ip route 10.1.10.0 255.255.255.0 10.1.2.2 90 track 1
ip route 10.1.15.0 255.255.255.0 10.1.1.2 90 track 2
ip route 3.3.3.3 255.255.255.255 GigabitEthernet0/0
ip route 10.1.10.0 255.255.255.0 10.1.1.2 100
ip route 10.1.15.0 255.255.255.0 10.1.2.2 100
```

Object Tracking on Switch 1

```
NME16Slot1# sh run | begin rtr 1
track 1 rtr 1 reachability
.
.
rtr 1
 type echo protocol ipIcmpEcho 10.1.1.1
 timeout 100
 frequency 3
rtr schedule 1 life forever start-time now
!
```

Object Tracking on Switch 2

```
NME16Slot2# sh run | begin rtr 1
track 1 rtr 1 reachability
.
.

rtr 1
 type echo protocol ipIcmpEcho 10.1.2.1
 timeout 100
 frequency 3
rtr schedule 1 life forever start-time now
!
```

DHCP Configuration on the Default Gateway

It is possible to assign IP addresses to the end user clients by defining DHCP pools for different subnets. DHCP is supported on both SMI and EMI images of Cisco Catalyst 3750 and 3560 distribution switches. The following configurations provide only an example. For further details on this feature, see the Cisco IOS configuration guide.

```
c3750-1#sh run | begin ip dhcp
ip dhcp pool phones
   network 10.1.20.0 255.255.255.0
   default-router 10.1.20.1
   option 150 ip 20.1.2.11
   dns-server 20.1.2.11
!
ip dhcp pool desktop
   network 10.1.30.0 255.255.255.0
   default-router 10.1.30.1
   dns-server 10.1.20.100
!
<Other configuration truncated>
```

Some IP addresses can be excluded from being assigned using the following command:

```
c3750-1(config)#ip dhcp excluded-address 10.1.20.1 10.1.20.5
```

Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is supported on Catalyst 3550, 3560, and 3750 switches. DAI is used to inspect all ARP request/response (gratuitous or non-gratuitous) coming from user-facing ports to ensure that they belong to the ARP owner. The ARP owner is the port that has a DHCP binding that matches the IP address contained in the ARP reply. ARP packets from the DAI trusted port are not inspected and are bridged to their respective VLANs. Dynamic ARP inspection is supported on access ports, trunk ports, EtherChannel ports, and private VLAN ports.

Follow these steps to configure DAI:

Step 1 Enable DHCP snooping on the VLANs:

```
c3750-1-1(config)#ip dhcp snooping
c3750-1-1(config)#ip dhcp snooping vlan 20,30
```

Step 2 Configure trusted ports (uplinks should be trusted ports):

```
c3750-1-1(config)#int po1
c3750-1-1(config-if)#ip arp inspection trust
```

```
c3750-1-1(config-if)#ip dhcp snooping trust
```

Step 3 Enable DAI on VLANs:

```
c3750-1-1(config)#ip arp inspection vlan 20,30 logging dhcp none
```

Step 4 Enable rate limit on physical ports:

```
c3750-1-1(config-if)#ip dhcp snooping limit rate 100
```

Step 5 Enable globally err disable caused by DAI:

```
c3750-1-1(config)#errdisable detect cause arp-inspection
```

Step 6 Enable the DAI logging feature ACL/DHCP-binding (for a full list of options and their meaning refer to the software configuration guide):

```
c3750-1-1(config)#ip arp inspection vlan 20,30 logging dhcp-bindings none
```

Step 7 Configure the DAI logging buffer to store deny/permit ARP packets:

```
c3750-1-1(config)#ip arp inspection log-buffer logs 1024 interval 60
```

Step 8 Configure DAI validation on the source and destination MAC IP addresses:

```
c3750-1-1(config)#ip arp inspection validate src-mac dst-mac ip
```

IP Source Guard

IP Source Guard (IPSG) is supported on Catalyst 3550, 3560, and 3750 switches. IPSG prevents traffic attacks caused by a spoofed IP address, and restricts IP traffic on Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database. In addition to dynamic IP source binding, IP source address bindings can be configured statically. Both IPSG and DAI depend on the DHCP snooping feature, and require that DHCP snooping be turned on. It is also possible to configure static bindings but this is not covered in this document.

```
c3750-1-1(config)#int f0/2
c3750-1-1(config-if)#ip verify source port-security
c3750-1-1(config-if)#end

c3750-1-1#show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  -------
---
Fa0/2      ip-mac       active       10.1.30.6        00:0F:20:C9:D9:9C  30
Fa0/2      ip-mac       active       10.1.20.2        00:30:94:C3:48:2E  20
c3750-1-1#
```

Note Both IPSG and DAI depend on enabling DHCP snooping in dynamic environments such as DHCP. See the DAI section to configure DHCP snooping. Without DHCP snooping, IPSG and DAI cause problems in normal traffic.

Conclusion

Several architectures are discussed in this document. The Cisco EtherSwitch Service Module provides flexibility and useful features. The first two topologies for the small and medium branch office are similar except for the devices used at the edge layer. The CPU utilization on the edge layer can be reduced by deploying the distribution layer if higher switching capacity is desired, either in the form of the EtherSwitch Service Module or the external distribution layer.

This document recommends Layer 2 at the access layer. Layer 2 services provide a platform to make deployment of additional services easier. RSTP converges quickly and also simplifies the configuration by incorporating some Cisco proprietary features such as BackboneFast and UplinkFast.

High availability and scalability are provided with this architecture. Users are authenticated and authorized before they log on to the network, when they are connected either directly or via the Cisco IP phone. To protect against Layer 2 attacks, more protection can be provided by enabling Layer 2 security. The switches provide smart port macros and autoQoS to quickly enable the features necessary for a converged network.

All the models support the necessary features for a converged network. The architecture and the topologies discussed in this document provide a baseline architecture that can be used for branch LAN switching.

References

- Cisco AVVID Network Infrastructure Enterprise Quality of Service Design Guide—http://www.cisco.com/application/pdf/en/us/guest/netsol/ns17/c649/ccmigration_09186a00800d67ed.pdf
- Cisco Campus Network Design Guide—http://www.cisco.com/warp/public/779/largeent/it/ese/srnd.html
- Full Service Branch Design Guide—http://www.cisco.com/go/srnd
- Configuration guides
  - http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3560/
  - http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/
  - http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2970/
  - http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/
- Additional useful links
  - http://www-tac.cisco.com/Training/partner_bootcamps/lanswitching_partner/lectures/revised07/328,1,Catalyst 3550
  - http://www-tac.cisco.com/Training/bootcamps/advanced_lanswitching_bootcamp/lectures/module5/common-issues-day5.pdf

Appendix

Integrating with the Edge Layer

Table 3 provides a list of Ethernet network modules available on various ISRs.

Note This table does not include the next generation network module.

Table 3 Ethernet Network Modules for Various ISRs

Network Module		Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
Ethernet Switching Network Modules					
NM-16ESW	16-port 10/100 Cisco EtherSwitch Network Module	No	Yes	Yes	Yes
NM-16ESW-1GIG	16-port 10/100 Cisco EtherSwitch Network Module with 1 Gigabit Ethernet (1000BASE-T) port	No	Yes	Yes	Yes
NM-16ESW-PWR	16-port 10/100 Cisco EtherSwitch Network Module with in-line power support	No	Yes	Yes	Yes
NM-16ESW-PWR-1GIG	16-port 10/100 Cisco EtherSwitch Network Module with in-line power and Gigabit Ethernet	No	Yes	Yes	Yes
NMD-36ESW	36-port 10/100 Cisco EtherSwitch High-Density Services Module (HDSM)	No	No	No	Yes
NMD-36ESW-2GIG	36-port 10/100 Cisco EtherSwitch HDSM with 1 Gigabit Ethernet (1000BASE-T) port	No	No	No	Yes
NMD-36ESW-PWR	36-port 10/100 Cisco EtherSwitch HDSM with in-line power support	No	No	No	Yes
NMD-36ESW-PWR-2G	36-port 10/100 Cisco EtherSwitch HDSM with in-line power and Gigabit Ethernet	No	No	No	Yes

Table 4 lists the ISR support for the Cisco EtherSwitch Service Module.

Table 4 Cisco EtherSwitch Service Module Support on Various ISRs

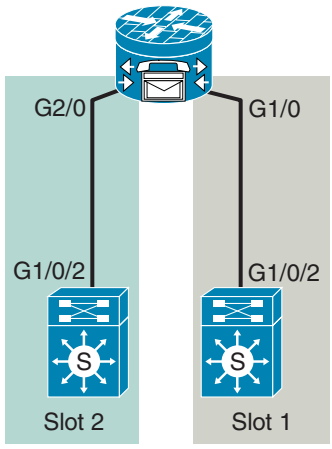
Module	Ports	Supported Platforms/Number per Platform	Maximum Powered Ports per Card
NME-16ES-1G-P	• 16x10/100 RJ-45 • 1x10/100/1000 RJ-45	• Cisco 2691/1 • Cisco 3725/2 • Cisco 3745/2 • Cisco 2811/1 • Cisco 2821/1 • Cisco 2851/1 • Cisco 3825/2 • Cisco 3845/2	16
NME-X-23ES-1G-P	• 23x10/100 RJ-45 • 1x10/100/1000 RJ-45	• Cisco 2821/1 • Cisco 2851/1 • Cisco 3825/1 • Cisco 3845/2	24
NME-XD-24ES-1S-P	• 24x10/100 RJ-45 • 1x SFP-based Gigabit Ethernet • 2x StackWise	• Cisco 2851/1 • Cisco 3825/1 • Cisco 3845/1	24
NME-XD-48ES-2S-P	• 48-10/100 RJ-45 • 2x SFP-based Gigabit Ethernet	• Cisco 2851/1 • Cisco 3825/1 • Cisco 3845/2	48

Note Cisco EtherSwitch Service Modules are the next generation switches supported in ISRs.

EtherSwitch and ISR Internal Connectivity Details

To establish a session, the Gigabit Ethernet link on the ISR must be configured with an IP address for console access to the network module. The details of connectivity between the ISR and the network module are shown in Figure 16.

Figure 16 Internal Interfaces of ISR and Network Modules



Cisco 3845 ISR with 2 NME-16ES-1G-P

When the network module is inserted into a slot (slot 1 of the Cisco 3845 in this example), the interface GigabitEthernet 1/0 on the ISR connects to the GigabitEthernet interface 1/0/2 of the network module. In a similar way, when in slot 2, the network modules GigabitEthernet interface 1/0/2 connects to GigabitEthernet 2/0 of the ISR. The network modules can be configured by establishing a session from the ISR to the network modules. To establish the session, an IP address must be assigned to the GigabitEthernet interfaces connecting to the network modules, and the interface brought up by entering the **no shut** command on the interface.