

TechNote: Netgear 7300 Series Level 3 Switch Sample Configurations

Netgear, Inc.

This TechNote provides examples of the use of the 7300 Series Level 3 Managed Switch in typical network settings.

This TechNote describes the use and advantages of specific functions provided by the 7300 Series L3 Switch, and will include instructions on how to configure those functions using the Command Line Interface and Graphical User Interface.

1.0 Functions Supported by the 7300 Series Level 3 Managed Switch

The available functions include:

⊙ **Layer 2 Switching:**

- Bridging support (the default) for IEEE 802.1D -- Spanning Tree plus IEEE 802.1w -- Rapid Reconfiguration and IEEE 802.1s -- Multiple Spanning Tree
- Virtual LAN (VLAN) operation conforming to IEEE 802.1Q, including Generic Attribute Registration Protocol (GARP), GARP Multicast Registration Protocol (GMRP) and GARP VLAN Registration Protocol (GVRP)
- Support for extensions to the Ethernet protocol:
 - VLAN tagging, required for VLAN support (formerly IEEE 802.3ac, now included in IEEE 802.3-2002)
 - Link Aggregation, which you may choose to implement to improve bandwidth and reliability for critical connections (formerly IEEE 802.3ad)
 - Flow Control at the MAC layer: you may configure the switch or a port to temporarily halt traffic when necessary to prevent overload (formerly IEEE 802.3x)
 - Additional functions you can use to manage the network including IGMP Snooping, Port Mirroring and Broadcast Storm Recovery

- ◎ **Layer 3 Routing**

- Base routing protocols, including support for the Address Resolution Protocol (ARP), IP Mapping, the Internet Control Message Protocol (ICMP) and Classless Inter-Domain Routing (CIDR)
- Support for protocols used by routers to exchange network topology information:
 - Routing Information Protocol (RIP) versions 1 and 2, recommended for use in small to medium sized networks
 - Open Shortest Path First (OSPF) version 2, used in larger, more complex networks
- Support for the Virtual Router Redundancy Protocol (VRRP) used to improve the reliability of network connections
- Support for the MD5 Message-Digest Algorithm defined in RFC 1321 used for digital signature applications
- Support for the use of Dynamic Host Configuration Protocol (DHCP) to assign IP addresses, including the Relay Agent Information option defined in RFC 3046

- ◎ **VLAN Routing:** Allows traffic received on a VLAN port to be processed by the Layer 3 routing function

- ◎ **Quality of Service**

- Access Control Lists, used to control access to specified resources
- Differentiated Services, which you can use to define traffic classes and how they will be treated, including traffic acceptance, transmission and bandwidth guarantees

1.1 Functions Described In This Document

This document includes examples of how to configure your 7300 Series L3 Switch in some typical network scenarios. The examples begin with support for port routing in a simple network, and explain how to activate the most common routing protocols. A discussion of the use of VLANs with and without VLAN routing is followed by sections on Link Aggregation and Virtual Router Redundancy Protocol. The document concludes with an introduction to the use of Access Control Lists and Differentiated Services.

2.0 Routing

The first networks were small enough for the end stations to communicate directly. As networks grew, Layer 2 bridging was used to segregate traffic, a technology that worked well for unicast traffic, but had problems coping with large quantities of multicast packets. The next major development was routing, where packets were examined and redirected at Layer 3. End stations needed to know how to reach their nearest router, and the routers had to understand the network topology so that they could forward traffic. Although bridges tended to be faster than routers, using routers allowed the network to be partitioned into logical subnetworks, which restricted multicast traffic and also facilitated the development of security mechanisms.

An end station specifies the destination station's Layer 3 address in the packet's IP header, but sends the packet to the MAC address of a router. When the Layer 3 router receives the packet, it will minimally:

- ⊙ Look up the Layer 3 address in its address table to determine the outbound port
- ⊙ Update the Layer 3 header
- ⊙ Recreate the Layer 2 header

The router's IP address is often statically configured in the end station, although the 7300 Series L3 Switch supports protocols such as DHCP that allow the address to be assigned dynamically. Likewise, you may assign some of the entries in the routing tables used by the router statically, but protocols such as RIP and OSPF allow the tables to be created and updated dynamically as the network configuration changes.

2.1 Port Routing Configuration

The 7300 Series L3 Switch always supports Layer 2 bridging, but Layer 3 routing must be explicitly enabled, first for the 7300 Series L3 Switch as a whole, and then for each port which is to participate in the routed network.

The configuration commands used in the example in this section enable IP routing on ports 0.2, 0.3, and 0.5. The router ID will be set to the 7300 Series L3 Switch's management IP address, or to that of any active router interface if the management address is not configured.

After the routing configuration commands have been issued, the following functions will be active:

- ⊙ IP Forwarding, responsible for forwarding received IP packets.
- ⊙ ARP Mapping, responsible for maintaining the ARP Table used to correlate IP and MAC addresses. The table contains both static entries and entries dynamically updated based on information in received ARP frames.
- ⊙ Routing Table Object, responsible for maintaining the common routing table used by all registered routing protocols.

You may then activate RIP or OSPF, used by routers to exchange route information, on top of IP Routing. RIP is more often used in smaller networks, while OSPF was designed for larger and more complex topologies.

2.1.1 Port Routing Configuration Example

The diagram in this section shows a Layer 3 switch configured for port routing. It connects three different subnets, each connected to a different port. The script shows the commands you would use to configure a 7300 Series L3 Switch to provide the port routing support shown in the diagram.

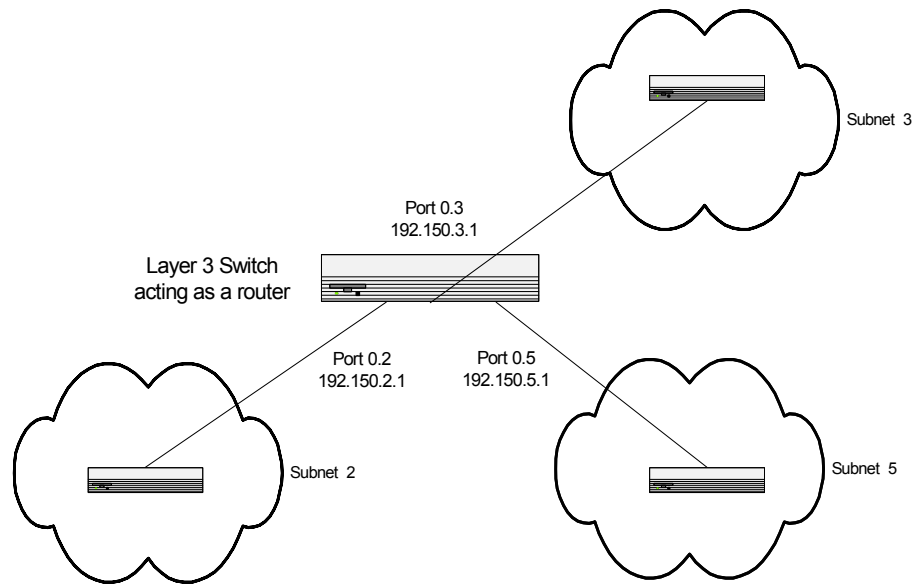


FIGURE 1. Port routing example network diagram

Table 1. Example of configuring port routing on a 7300 Series L3 Switch

Routing
<p><i>Enable routing for the switch. IP forwarding will then be enabled by default.</i></p> <pre>config routing enable</pre> <p><i>Enable routing for three of the ports on the switch. The default link-level encapsulation format will be Ethernet.</i></p> <pre>config interface routing 0.2 enable config interface routing 0.3 enable config interface routing 0.5 enable</pre> <p><i>Configure the IP addresses and subnet masks for the ports. Network directed broadcast frames will be dropped and the maximum transmission unit size will be 1500 bytes.</i></p> <pre>config ip interface create 0.2 192.150.2.1 255.255.255.0 config ip interface create 0.3 192.150.3.1 255.255.255.0 config ip interface create 0.5 192.150.5.1 255.255.255.0</pre>

Use the following screens to perform the same configuration using the Graphical User Interface:

- Ⓞ **Routing --> IP --> Configuration.** To enable routing for the switch.
- Ⓞ **Routing --> IP --> Interface Configuration.** For the remaining commands.

2.2 RIP Configuration

Routing Information Protocol (RIP) is one of the protocols which may be used by routers to exchange network topology information. It is characterized as an “interior” gateway protocol, and is typically used in small to medium-sized networks.

A router running RIP will send the contents of its routing table to each of its adjacent routers every 30 seconds. When a route is removed from the routing table it will be flagged as unusable by the receiving routers after 180 seconds, and removed from their tables after an additional 120 seconds.

There are two versions of RIP:

- ⊙ RIPv1 defined in RFC 1058
 - Routes are specified by IP destination network and hop count
 - The routing table is broadcast to all stations on the attached network
- ⊙ RIPv2 defined in RFC 1723
 - Route specification is extended to include subnet mask and gateway
 - The routing table is sent to a multicast address, reducing network traffic
 - An authentication method is used for security

The 7300 Series Level 3 Managed Switch supports both versions of RIP. You may configure a given port to:

- ⊙ Receive packets in either or both formats
- ⊙ Transmit packets formatted for RIPv1 or RIPv2 or to send RIPv2 packets to the RIPv1 broadcast address
- ⊙ Prevent any RIP packets from being received
- ⊙ Prevent any RIP packets from being transmitted

2.2.1 RIP Configuration Example

The configuration commands used in the following example enable RIP on ports 0.2 and 0.3.

Table 2. Example of configuring RIP on a 7300 Series L3 Switch operating as a router

RIP
<pre>Enable routing for the switch and ports 0.2 and 0.3. config routing enable config interface routing 0.2 enable config interface routing 0.3 enable config ip interface create 0.2 192.150.2.1 255.255.255.0 config ip interface create 0.3 192.150.3.1 255.255.255.0 Enable RIP for the switch. The route preference will default to 15. config router id 192.150.9.9 config router rip adminmode enable Enable RIP for ports 0.2 and 0.3. Authentication will default to none, and no default route entry will be created. config router rip interface mode 0.2 enable config router rip interface mode 0.3 enable Specify that both ports will receive both RIPv1 and RIPv2 frames, but will send only RIPv2 formatted frames. config router rip interface version receive 0.2 both config router rip interface version receive 0.3 both config router rip interface version send 0.2 rip2 config router rip interface version send 0.3 rip2</pre>

Use the following screens to perform the same configuration using the Graphical User Interface:

- ⦿ **Routing --> IP --> Configuration.** To enable routing for the switch and specify the router ID.
- ⦿ **Routing --> IP --> Interface Configuration.** To enable routing for the ports and configure their IP addresses and subnet masks.
- ⦿ **Routing --> RIP --> Configuration.** To enable RIP for the switch.
- ⦿ **Routing --> RIP --> Interface Configuration.** To enable RIP for the ports and specify the RIP versions.

2.3 OSPF Configuration

For larger networks Open Shortest Path First (OSPF) is generally used in preference to RIP. OSPF offers several benefits to the administrator of a large and/or complex network:

- ⦿ Less network traffic:
 - Routing table updates are sent only when a change has occurred
 - Only the part of the table which has changed is sent

-
- Updates are sent to a multicast, not a broadcast, address
 - ⊙ Hierarchical management, allowing the network to be subdivided

The top level of the hierarchy of an OSPF network is known as an autonomous system (AS) or routing domain, and is a collection of networks with a common administration and routing strategy. The AS is divided into areas: intra-area routing is used when a source and destination address are in the same area, and inter-area routing across an OSPF backbone is used when they are not. An inter-area router communicates with border routers in each of the areas to which it provides connectivity.

The 7300 Series L3 Switch operating as a router and running OSPF will determine the best route using the assigned cost and the type of the OSPF route. The order for choosing a route if more than one type of route exists is as follows:

- ⊙ Intra-area
- ⊙ Inter-area
- ⊙ External type 1: the route is external to the AS
- ⊙ External Type 2: the route was learned from other protocols such as RIP

2.3.1 OSPF Configuration Examples

The examples in this section show you how to configure a 7300 Series L3 Switch first as an inter-area router and then as a border router. They show two areas, each with its own border router connected to one inter-area router.

The first diagram shows a network segment with an inter-area router connecting areas 0.0.0.2 and 0.0.0.3. The example script shows the commands used to configure a 7300 Series L3 Switch as the inter-area router in the diagram by enabling OSPF on port 0.2 in area 0.0.0.2 and port 0.3 in area 0.0.0.3.

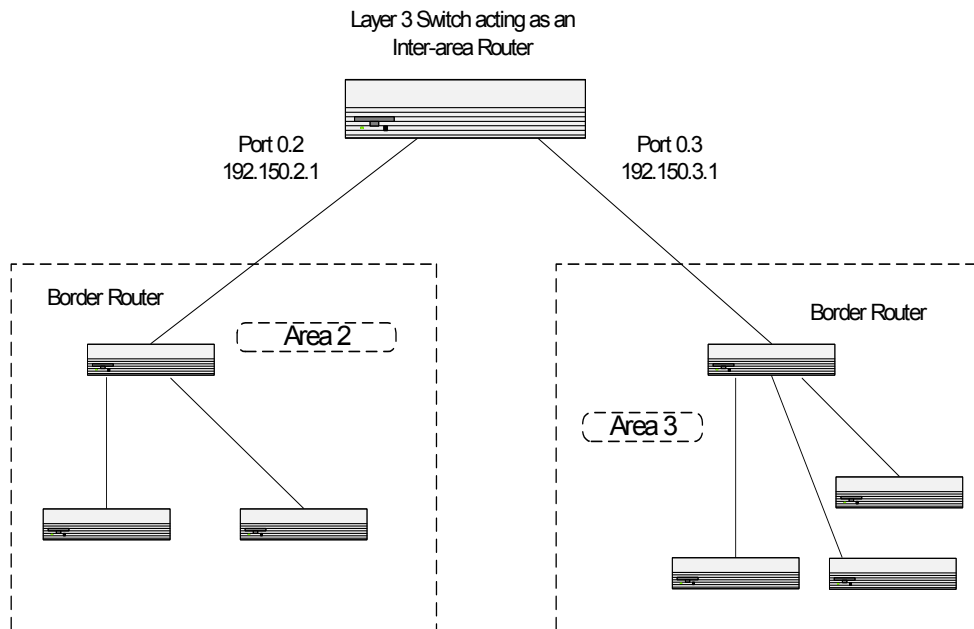


FIGURE 2. OSPF example network diagram: inter-area router

Table 3. Example of configuring OSPF on a 7300 Series L3 Switch operating as an inter-area router

OSPF: inter-area router
<pre> Enable routing for the switch and ports 0.2 and 0.3. config routing enable config interface routing 0.2 enable config interface routing 0.3 enable config ip interface create 0.2 192.150.2.1 255.255.255.0 config ip interface create 0.3 192.150.3.1 255.255.255.0 Specify the router ID and enable OSPF for the switch. config router id 192.150.9.9 config router ospf adminmode enable Enable OSPF for the ports. config router ospf interface areaid 0.2 0.0.0.2 config router ospf interface areaid 0.3 0.0.0.3 config router ospf interface mode 0.2 enable config router ospf interface mode 0.3 enable Set the OSPF priority and cost for the ports. config router ospf interface priority 0.2 128 config router ospf interface priority 0.3 255 config router ospf interface cost 0.2 32 config router ospf interface cost 0.3 64</pre>

- ⊙ Use the following screens to perform the same configuration using the Graphical User Interface:
- ⊙ **Routing --> IP --> Configuration.** To enable routing for the switch and specify the router ID.
- ⊙ **Routing --> IP --> Interface Configuration.** To enable routing for the ports and configure their IP addresses and subnet masks.
- ⊙ **Routing --> OSPF --> Info.** To enable OSPF for the switch.
- ⊙ **Routing --> OSPF--> Interface Configuration.** To enable OSPF for the ports and specify the priority and cost parameters.

The next diagram shows the same network segment with the 7300 Series L3 Switch operating as the border router in area 0.0.0.2. The example script shows the commands used to configure the switch with OSPF enabled on port 0.2 for communication with the inter-area router in the OSPF backbone, and on ports 0.3 and 0.4 for communication with subnets within area 0.0.0.2

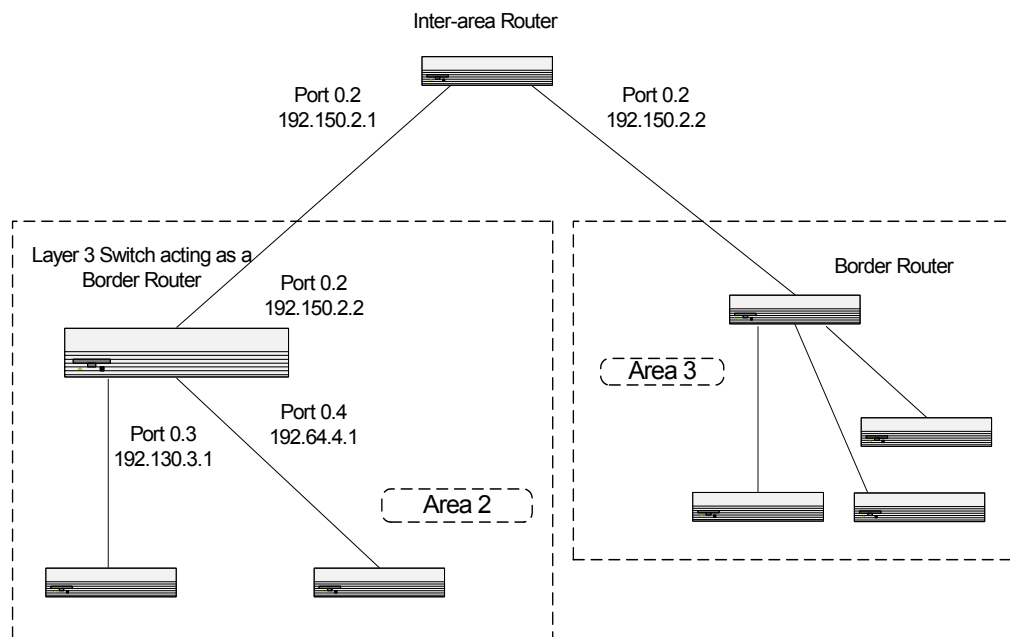


FIGURE 3. OSPF example network diagram: border router

Table 4. Example of configuring OSPF on a 7300 Series L3 Switch operating as a border router

OSPF: border router
<pre>Enable routing for the switch and ports 0.2, 0.3 and 0.4. config routing enable config interface routing 0.2 enable config interface routing 0.3 enable config interface routing 0.4 enable config ip interface create 0.2 192.150.2.2 255.255.255.0 config ip interface create 0.3 192.130.3.1 255.255.255.0 config ip interface create 0.4 192.64.4.1 255.255.255.0 Specify the router ID and enable OSPF for the switch. config router id 192.130.1.1 config router ospf adminmode enable Enable OSPF for the ports. config router ospf interface areaid 0.2 0.0.0.2 config router ospf interface areaid 0.3 0.0.0.2 config router ospf interface areaid 0.4 0.0.0.2 config router ospf interface mode 0.2 enable config router ospf interface mode 0.3 enable config router ospf interface mode 0.4 enable Set the OSPF priority and cost for the ports. config router ospf interface priority 0.2 128 config router ospf interface priority 0.3 255 config router ospf interface priority 0.4 255 config router ospf interface cost 0.2 32 config router ospf interface cost 0.3 64 config router ospf interface cost 0.4 64</pre>

Use the following screens to perform the same configuration using the Graphical User Interface:

- ⦿ **Routing --> IP --> Configuration.** To enable routing for the switch and specify the router ID.
- ⦿ **Routing --> IP --> Interface Configuration.** To enable routing for the ports and configure their IP addresses and subnet masks.
- ⦿ **Routing --> OSPF --> Info.** To enable OSPF for the switch.
- ⦿ **Routing --> OSPF--> Interface Configuration.** To enable OSPF for the ports and specify the priority and cost parameters.

3.0 Virtual LANs

Adding Virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast, and like a router, it partitions the network into logical seg-

ments, which provides better administration, security and management of multicast traffic.

A VLAN is a set of end stations and the switch ports that connect them. You may have many reasons for the logical division, such as department or project membership. The only physical requirement is that the end station and the port to which it is connected both belong to the same VLAN.

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station may omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet may either reject it or insert a tag using its default VLAN ID. A given port may handle traffic for more than one VLAN, but it can only support one default VLAN ID.

3.1 VLAN Configuration Example

The diagram in this section shows a 7300 Series L3 Switch with four ports configured to handle the traffic for two VLANs. Port 0.2 handles traffic for both VLANs, while port 0.1 is a member of VLAN 2 only, and ports 0.3 and 0.4 are members of VLAN 3 only. The script following the diagram shows the commands you would use to configure the switch as shown in the diagram.

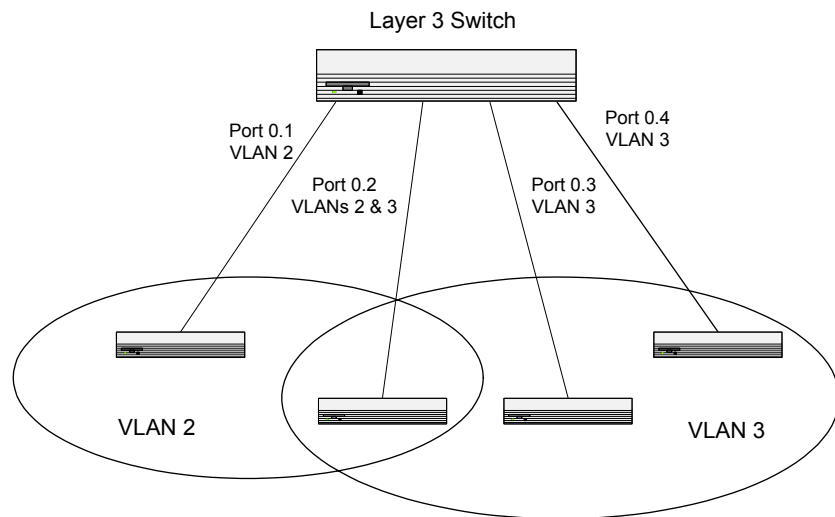


FIGURE 4. VLAN example network diagram

Table 5. Example of configuring VLAN support on a 7300 Series L3 Switch

VLAN
<p><i>Create two VLANs and assign the VLAN ids while leaving the names blank.</i></p> <pre>config vlan create 2 config vlan create 3</pre> <p><i>Assign the ports that will belong to VLAN 2, specify that frames will always be transmitted tagged from all member ports, and that untagged frames will be rejected on receipt.</i></p> <pre>config vlan participation include 2 0.1 config vlan participation include 2 0.2 config vlan port tagging enable 2 all config vlan port acceptframe vlanonly 0.1 config vlan port acceptframe vlanonly 0.2</pre> <p><i>Assign the ports that will belong to VLAN 3, note that port 0.2 belongs to both VLANs and that port 0.5 can never belong to VLAN 3. Specify that untagged frames will be accepted on ports 0.4 and 0.5.</i></p> <pre>config vlan participation include 3 0.2 config vlan participation include 3 0.3 config vlan participation include 3 0.4 config vlan participation exclude 3 0.5 config vlan port acceptframe all 0.4 config vlan port acceptframe all 0.5</pre> <p><i>Assign VLAN 3 as the default VLAN for port 0.2.</i></p> <pre>config vlan port pvid 3 0.2</pre>

Use the following screens to perform the same configuration using the Graphical User Interface:

- ⊙ **Switching --> VLAN--> Configuration.** To create the VLANs and specify port participation.
- ⊙ **Switching --> VLAN --> Port Configuration.** To specify the handling of untagged frames on receipt, and whether frames will be transmitted tagged or untagged.

4.0 VLAN Routing

You can configure a 7300 Series Level 3 Managed Switch with some ports supporting VLANs and some supporting routing. You can also configure it to allow traffic on a VLAN to be treated as if the VLAN were a router port.

When a port is enabled for bridging (the default) rather than routing, all normal bridge processing is performed for an inbound packet, which is then associated with a VLAN. Its MAC Destination Address (DA) and VLAN ID are used to search the MAC address table. If routing is enabled for the VLAN and the MAC DA of an inbound unicast packet is that of the internal bridge-router interface, the packet will be routed. An inbound multicast packet will be forwarded to all ports in the VLAN, plus the internal bridge-router interface if it was received on a routed VLAN.

Since a port can be configured to belong to more than one VLAN, VLAN routing might be enabled for all of the VLANs on the port, or for a subset. VLAN Routing can be used to allow more than one physical port to reside on the same subnet. It could also be used when a VLAN spans multiple physical networks, or when additional segmentation or security is required.

The next section will show you how to configure the 7300 Series Level 3 Managed Switch to support VLAN routing and how to use RIP and OSPF. A port may be either a VLAN port or a router port, but not both. However, a VLAN port may be part of a VLAN that is itself a router port.

4.1 VLAN Routing Configuration

This section provides an example of how to configure a 7300 Series L3 Switch to support VLAN routing. The configuration of the VLAN router port is similar to that of a physical port. The main difference is that, after the VLAN has been created, you must use the **show ip vlan** command to determine the VLAN's interface ID so that you can use it in the router configuration commands.

4.1.1 VLAN Routing Configuration Example

The diagram in this section shows a Layer 3 switch configured for port routing. It connects two VLANs, with two ports participating in one VLAN, and one port in the other. The script shows the commands you would use to configure a 7300 Series L3 Switch to provide the VLAN routing support shown in the diagram.

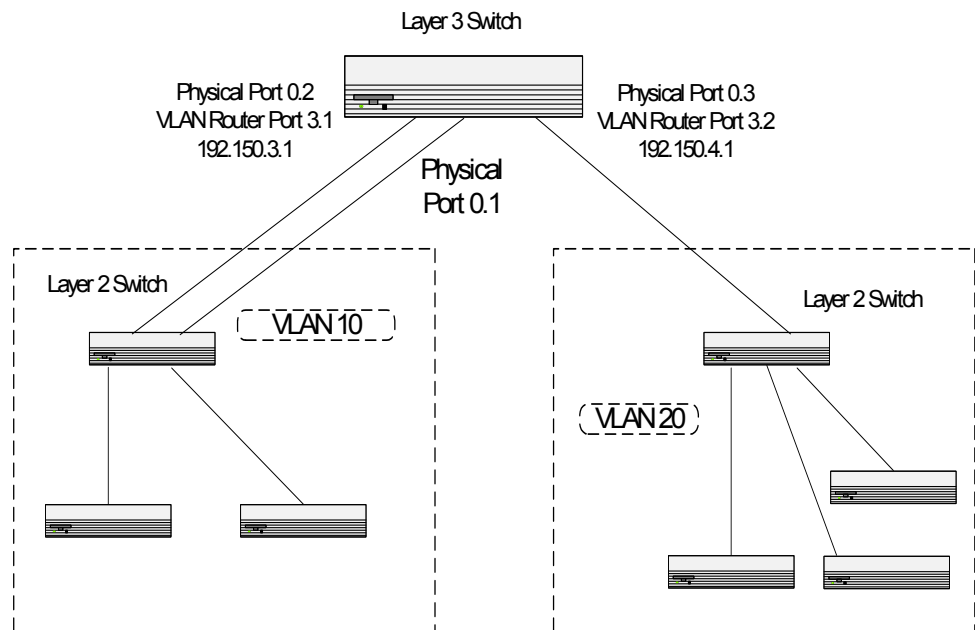


FIGURE 5. VLAN routing example network diagram

Table 6. Example of configuring VLAN Routing support on a 7300 Series L3 Switch

VLAN Routing
<pre>Create two VLANs with egress frame tagging enabled. config vlan create 10 config vlan create 20 config vlan participation include 10 0.1 config vlan participation include 10 0.2 config vlan participation include 20 0.3 config vlan port tagging enable 10 all config vlan port tagging enable 20 all Specify the VLAN ID assigned to untagged frames received on the ports. config vlan port pvid 10 0.1 config vlan port pvid 10 0.2 config vlan port pvid 20 0.3 Enable routing for the VLANs. config ip vlan routing create 10 config ip vlan routing create 20 show ip vlan This will return the logical interface IDs that will be used instead of slot.port in subsequent routing commands. Assume that VLAN 10 is assigned ID 3.1 and VLAN 20 is assigned ID 3.2. Enable routing for the switch. config routing enable Configure the IP addresses and subnet masks for the virtual router ports. config ip interface create 3.1 192.150.3.1 255.255.255.0 config ip interface create 3.2 192.150.4.1 255.255.255.0</pre>

Use the following screens to perform the same configuration using the Graphical User Interface:

- ⦿ **Switching --> VLAN--> Configuration.** To create the VLANs and specify port participation.
- ⦿ **Switching --> VLAN --> Port Configuration.** To specify the handling of untagged frames on receipt, and whether frames will be transmitted tagged or untagged.
- ⦿ **Routing --> VLAN Routing --> Configuration.** To enable VLAN routing and configure the ports.
- ⦿ **Routing --> IP --> Configuration.** To enable routing for the switch.
- ⦿ **Routing --> IP --> Interface Configuration.** To enable routing for the ports and configure their IP addresses and subnet masks.

4.2 VLAN Routing RIP Configuration

Routing Information Protocol (RIP) is one of the protocols which may be used by routers to exchange network topology information. It is characterized as an “interior” gateway protocol, and is typically used in small to medium-sized networks.

A router running RIP will send the contents of its routing table to each of its adjacent routers every 30 seconds. When a route is removed from the routing table it will be flagged as unusable by the receiving routers after 180 seconds, and removed from their tables after an additional 120 seconds.

There are two versions of RIP:

- RIPv1 defined in RFC 1058
- Routes are specified by IP destination network and hop count
- The routing table is broadcast to all stations on the attached network
- ⊙ RIPv2 defined in RFC 1723
 - Route specification is extended to include subnet mask and gateway
 - The routing table is sent to a multicast address, reducing network traffic
 - An authentication method is used for security

The 7300 Series Level 3 Managed Switch supports both versions of RIP. You may configure a given port:

- ⊙ To receive packets in either or both formats
- ⊙ To transmit packets formatted for RIPv1 or RIPv2 or to send RIPv2 packets to the RIPv1 broadcast address
- ⊙ To prevent any RIP packets from being received
- ⊙ To prevent any RIP packets from being transmitted.

4.2.1 VLAN Routing RIP Configuration Example

This example adds support for RIPv2 to the configuration created in the base VLAN routing example. A second router, using port routing rather than VLAN routing, has been added to the network.

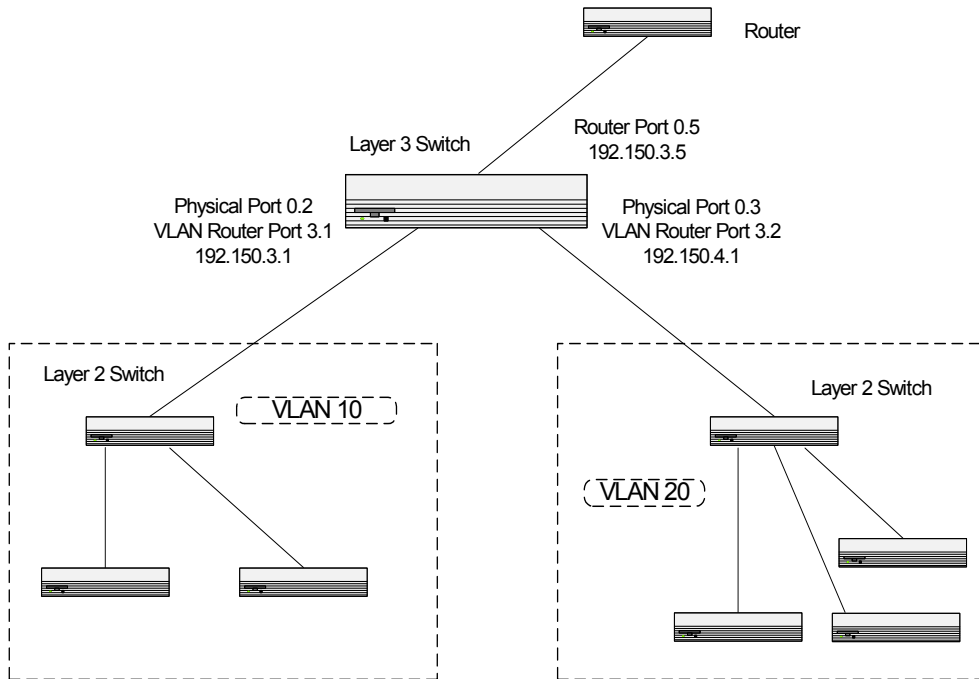


FIGURE 6. RIPv2 for VLAN routing example network diagram

Table 7. Example of configuring VLAN Routing with RIP support on a 7300 Series L3 Switch

RIP for VLAN Routing
<pre>Create the VLANs and enable VLAN routing. config vlan create 10 config vlan create 20 config vlan participation include 10 0.2 config vlan participation include 20 0.3 config vlan port tagging enable 10 all config vlan port tagging enable 20 all config vlan port pvid 10 0.2 config vlan port pvid 20 0.3 config ip vlan routing create 10 config ip vlan routing create 20 show ip vlan config routing enable config ip interface create 3.1 192.150.3.1 255.255.255.0 config ip interface create 3.2 192.150.4.1 255.255.255.0 Enable RIP for the switch. The route preference will default to 15. config router id 192.150.9.9 config router enable Configure the IP address and subnet mask for a non-virtual router port. config ip interface create 0.5 192.150.3.5 255.255.255.0 Enable RIP for the VLAN router ports. Authentication will default to none, and no default route entry will be created. config router rip interface mode 3.1 enable config router rip interface mode 3.2 enable</pre>

Use the following screens to perform the same configuration using the Graphical User Interface:

- ⊙ **Switching --> VLAN--> Configuration.** To create the VLANs and specify port participation.
- ⊙ **Switching --> VLAN --> Port Configuration.** To specify the handling of untagged frames on receipt, and whether frames will be transmitted tagged or untagged.
- ⊙ **Routing --> VLAN Routing --> Configuration.** To enable VLAN routing and configure the ports.
- ⊙ **Routing --> IP --> Configuration.** To enable routing for the switch and specify the router ID.
- ⊙ **Routing --> IP --> Interface Configuration.** To enable routing for the ports and configure their IP addresses and subnet masks.
- ⊙ **Routing --> RIP --> Configuration.** To enable RIP for the switch.

-
-
- ⊙ **Routing --> RIP --> Interface Configuration.** To enable RIP for the ports and specify the RIP versions.

4.3 VLAN Routing OSPF Configuration

For larger networks Open Shortest Path First (OSPF) is generally used in preference to RIP. OSPF offers several benefits to the administrator of a large and/or complex network:

Less network traffic:

- ⊙ Routing table updates are sent only when a change has occurred
- ⊙ Only the part of the table which has changed is sent
- ⊙ Updates are sent to a multicast, not a broadcast, address
- ⊙ Hierarchical management, allowing the network to be subdivided

The top level of the hierarchy of an OSPF network is known as an autonomous system (AS) or routing domain, and is a collection of networks with a common administration and routing strategy. The AS is divided into areas: intra-area routing is used when a source and destination address are in the same area, and inter-area routing across an OSPF backbone is used when they are not. An inter-area router communicates with border routers in each of the areas to which it provides connectivity.

The 7300 Series L3 Switch operating as a router and running OSPF will determine the best route using the assigned cost and the type of the OSPF route. The order for choosing a route if more than one type of route exists is as follows:

- ⊙ Intra-area
- ⊙ Inter-area
- ⊙ External type 1: the route is external to the AS
- ⊙ External Type 2: the route was learned from other protocols such as RIP

4.3.1 VLAN Routing OSPF Configuration Example

This example adds support for OSPF to the configuration created in the base VLAN routing example. The script shows the commands you would use to configure the 7300 Series L3 Switch as an inter-area router.

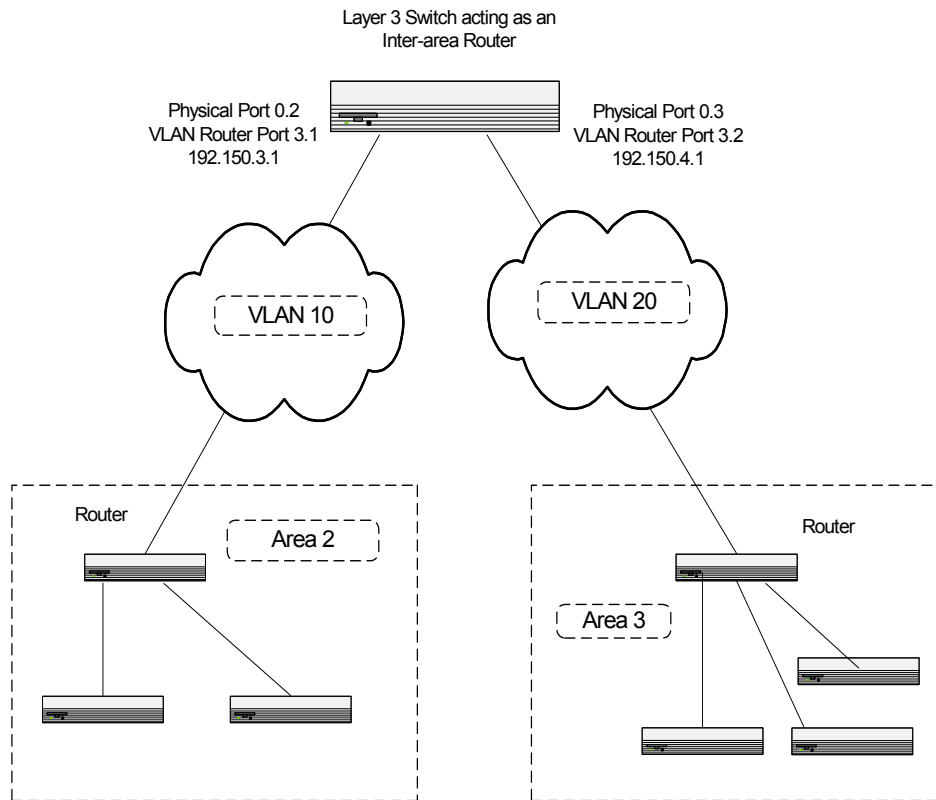


FIGURE 7. Example of configuring OSPF on a 7300 Series L3 Switch acting as an inter-area router running VLAN routing

Table 8. Example of configuring VLAN Routing with OSPF support on a 7300 Series L3 Switch

OSPF for VLAN Routing
<pre>Create the VLANs and enable VLAN routing. config vlan create 10 config vlan create 20 config vlan participation include 10 0.2 config vlan participation include 20 0.3 config vlan port tagging enable 10 all config vlan port tagging enable 20 all config vlan port pvid 10 0.2 config vlan port pvid 20 0.3 config ip vlan routing create 10 config ip vlan routing create 20 show ip vlan config routing enable config ip interface create 3.1 192.150.3.1 255.255.255.0 config ip interface create 3.2 192.150.4.1 255.255.255.0 Specify the router ID and enable OSPF for the switch. config router id 192.150.9.9 config router ospf adminmode enable Enable OSPF for the VLAN and physical router ports. config router ospf interface areaid 3.1 0.0.0.2 config router ospf interface areaid 3.2 0.0.0.3 config router ospf interface mode 3.1 enable config router ospf interface mode 3.2 enable Set the OSPF priority and cost for the VLAN and physical router ports. config router ospf interface priority 3.1 128 config router ospf interface priority 3.2 255 config router ospf interface cost 3.1 32 config router ospf interface cost 3.2 64</pre>

Use the following screens to perform the same configuration using the Graphical User Interface:

- ⊙ **Switching --> VLAN--> Configuration.** To create the VLANs and specify port participation.
- ⊙ **Switching --> VLAN --> Port Configuration.** To specify the handling of untagged frames on receipt, and whether frames will be transmitted tagged or untagged.
- ⊙ **Routing --> VLAN Routing --> Configuration.** To enable VLAN routing and configure the ports.
- ⊙ **Routing --> IP --> Configuration.** To enable routing for the switch and specify the router ID.

-
- ⊙ **Routing --> IP --> Interface Configuration.** To enable routing for the ports and configure their IP addresses and subnet masks.
 - ⊙ **Routing --> OSPF --> Info.** To enable OSPF for the switch.
 - ⊙ **Routing --> OSPF--> Interface Configuration.** To enable OSPF for the ports and specify the priority and cost parameters.

5.0 Link Aggregation

Link Aggregation (LAG) allows multiple physical links between two end-points to be treated as a single logical link. All of the physical links in a given LAG must operate in full-duplex mode at the same speed.

Link Aggregation is often used to directly connect two switches when the traffic between them requires high bandwidth and reliability, or to provide a higher bandwidth connection to a public network. LAG can offer the following benefits:

- ⊙ Increased reliability and availability -- if one of the physical links in the LAG goes down, traffic will be dynamically and transparently reassigned to one of the other physical links
- ⊙ Better use of physical resources -- traffic can be load-balanced across the physical links
- ⊙ Increased bandwidth -- the aggregated physical links deliver higher bandwidth than each individual link.
- ⊙ Incremental increase in bandwidth -- LAG may be used when a physical upgrade would produce a 10-times increase in bandwidth, but only a two- or five-times increase is required.

A LAG will be treated by management functions as if it were a single physical port. It may be included in a VLAN. More than one LAG may be configured for a given switch.

5.1 Link Aggregation Configuration Example

This section provides an example of configuring the 7300 Series Level 3 Managed Switch to support Link Aggregation (LAG) to a server and to a Layer 2 switch.

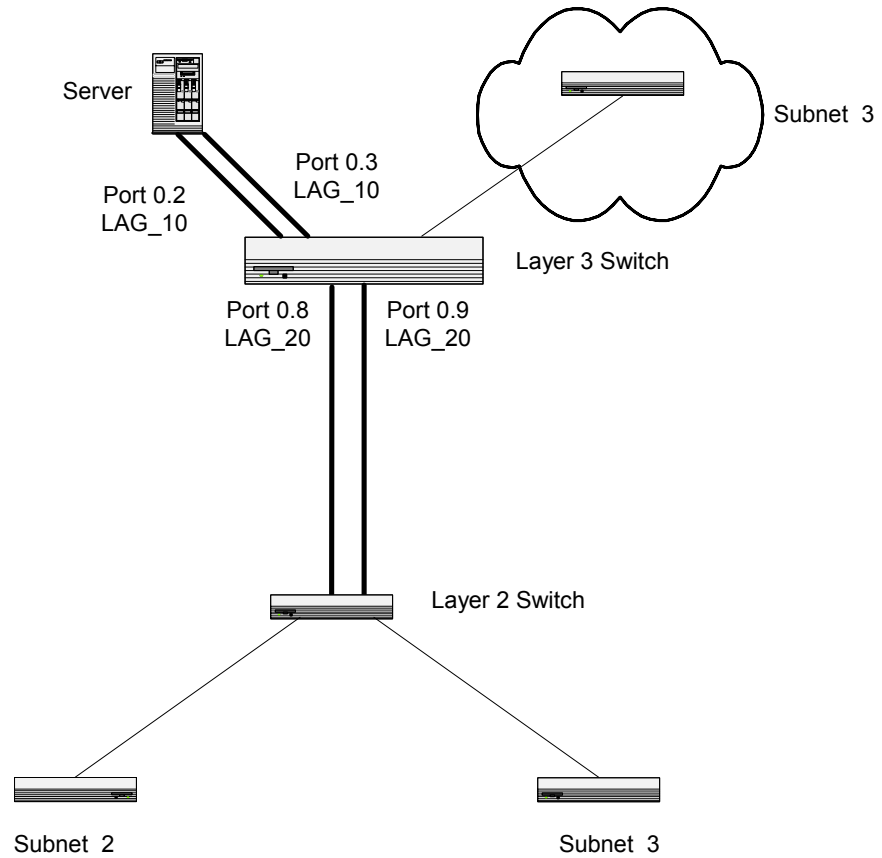


FIGURE 8. LAG example network diagram

Table 9. Example of configuring LAG support on a 7300 Series L3 Switch

LAG
<pre>Create two LAGs. config lag create lag_10 config lag create lag_20 show lag all This command will return the logical interface ids that will be used to identify the LAGs in subsequent commands. Assume that lag_10 is assigned id 1.1 and lag_20 is assigned id 1.2. Add the ports to the appropriate LAG. config lag addport 1.1 0.2 config lag addport 1.1 0.3 config lag addport 1.2 0.8 config lag addport 1.2 0.9 Enable both LAGs. Link trap notification will be enabled by default, and STP mode will be set to IEEE 802.1D-compliant. config lag adminmode all enable At this point the LAGs could be added to VLANs.</pre>

Use the following screen to perform the same configuration using the Graphical User Interface:

Switching --> Link Aggregation --> Configuration. To create the LAGs, specify port participation and enable LAG support on the switch.

6.0 Virtual Router Redundancy Protocol

When an end station is statically configured with the address of the router that will handle its routed traffic, a single point of failure is introduced into the network. If the router goes down, the end station is unable to communicate. Since static configuration is a convenient way to assign router addresses, Virtual Router Redundancy Protocol (VRRP) was developed to provide a backup mechanism.

VRRP eliminates the single point of failure associated with static default routes by enabling a backup router to take over from a “master” router without affecting the end stations using the route. The end stations will use a “virtual” IP address that will be recognized by the backup router if the master router fails. Participating routers use an election protocol to determine which router is the master router at any given time. A given port may appear as more than one virtual router to the network, also, more than one port on a 7300 Series L3 Switch may be configured as a virtual router. Either a physical port or a routed VLAN may participate.

6.1 Virtual Router Redundancy Protocol Configuration Example

This example shows how to configure the 7300 Series L3 Switch to support VRRP. Router 1 will be the default master router for the virtual route, and Router 2 will be the backup router.

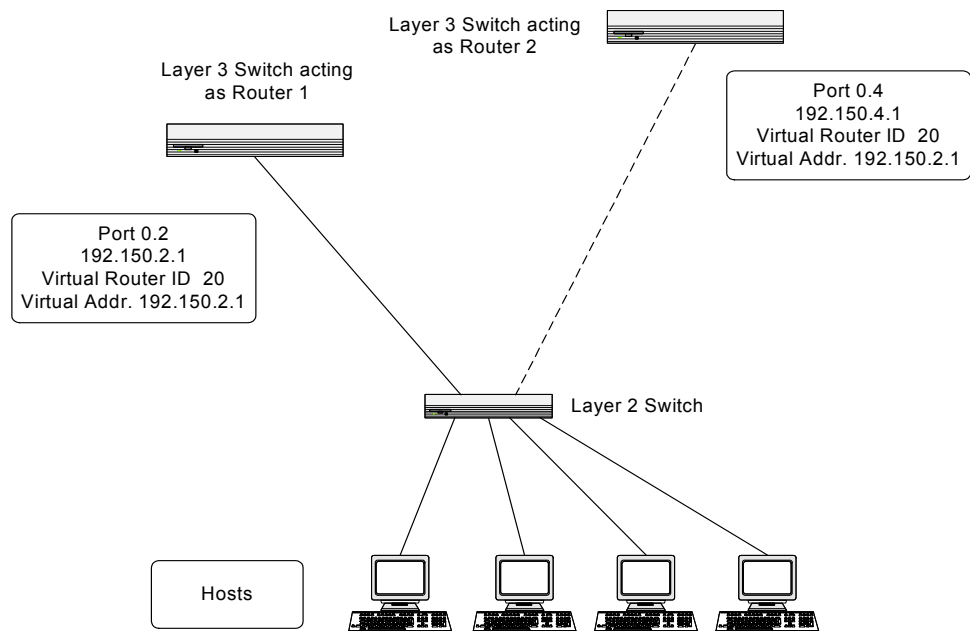


FIGURE 9. VRRP example network configuration

Table 10. Example of configuring VRRP on a 7300 Series L3 Switch acting as the master router

VRRP: master router (Router 1)
<p><i>Enable routing for the switch. IP forwarding will then be enabled by default.</i></p> <pre>config routing enable</pre>
<p><i>Configure the IP addresses and subnet masks for the port that will participate in the protocol.</i></p> <pre>config ip interface create 0.2 192.150.2.1 255.255.255.0</pre>
<p><i>Enable VRRP for the switch.</i></p> <pre>config router vrrp adminmode enable</pre>
<p><i>assign virtual router IDs to the port that will participate in the protocol.</i></p> <pre>config router vrrp interface routerID 0.2 20</pre>
<p><i>Specify the IP address that the virtual router function will recognize. Note that the virtual IP address on port 0.2 is the same as the port's actual IP address, therefore this router will always be the VRRP master when it is active.</i></p> <pre>config router vrrp interface ipaddress 0.2 192.150.2.1</pre>
<p><i>Set the priority for the port. Port 0.2 must be set to 255 because it is the IP address owner.</i></p> <pre>config router vrrp interface priority 0.2 20 255</pre>
<p><i>Enable VRRP on the port.</i></p> <pre>config router vrrp interface adminmode 0.2 20 enable</pre>

Table 11. Example of configuring VRRP on a 7300 Series L3 Switch acting as the backup router

VRRP: backup router (Router 2)
<p><i>Enable routing for the switch. IP forwarding will then be enabled by default.</i></p> <pre>config routing enable</pre>
<p><i>Configure the IP addresses and subnet masks for the port that will participate in the protocol.</i></p> <pre>config ip interface create 0.4 192.150.4.1 255.255.255.0</pre>
<p><i>Enable VRRP for the switch.</i></p> <pre>config router vrrp adminmode enable</pre>
<p><i>Assign virtual router IDs to the port that will participate in the protocol.</i></p> <pre>config router vrrp interface routerID 0.4 20</pre>
<p><i>Specify the IP address that the virtual router function will recognize. Since the virtual IP address on port 0.4 is the same as Router 1's port 0.2 actual IP address, this router will always be the VRRP backup when Router 1 is active.</i></p> <pre>config router vrrp interface ipaddress 0.4 192.150.2.1</pre>
<p><i>Set the priority for the port.</i></p> <pre>config router vrrp interface priority 0.4 20 255</pre>
<p><i>Enable VRRP on the port.</i></p> <pre>config router vrrp interface adminmode 0.4 20 enable</pre>

Use the following screens to perform the same configuration using the Graphical User Interface:

- ⊙ **Routing --> IP --> Configuration.** To enable routing for the switch.
- ⊙ **Routing --> IP --> Interface Configuration.** To enable routing for the ports and configure their IP addresses and subnet masks.
- ⊙ **Routing --> VRRP --> VRRP Configuration.** To enable VRRP for the switch
- ⊙ **Routing --> VRRP --> Virtual Router Configuration.** To complete the configuration.

7.0 Access Control Lists

Access Control Lists (ACLs) are used to control the traffic entering a network: they are normally used in a firewall router or in a router connecting two internal networks. You may selectively admit or reject inbound traffic, thereby controlling access to your network, or to specific resources on your network.

Each ACL is a set of one to ten rules applied to inbound traffic. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network, and may apply to one or more of the following six fields within a packet:

- ⊙ Source IP address
- ⊙ Destination IP address

- ⊙ Source Layer 4 port
- ⊙ Destination Layer 4 port
- ⊙ TOS byte
- ⊙ Protocol number

Note: The order of the rules is important. When a packet matches multiple rules, the first rule takes precedence. Also, once you define an ACL for a given port, all traffic not specifically permitted by the ACL will be denied access.

7.1 Access Control List Configuration Example

The script in this section shows you how to set up an ACL with two rules, one applicable to TCP traffic and one to UDP traffic. The content of the two rules is the same. TCP and UDP packets will only be accepted by the 7300 Series L3 Switch if the source and destination stations have IP addresses that fall within the defined sets.

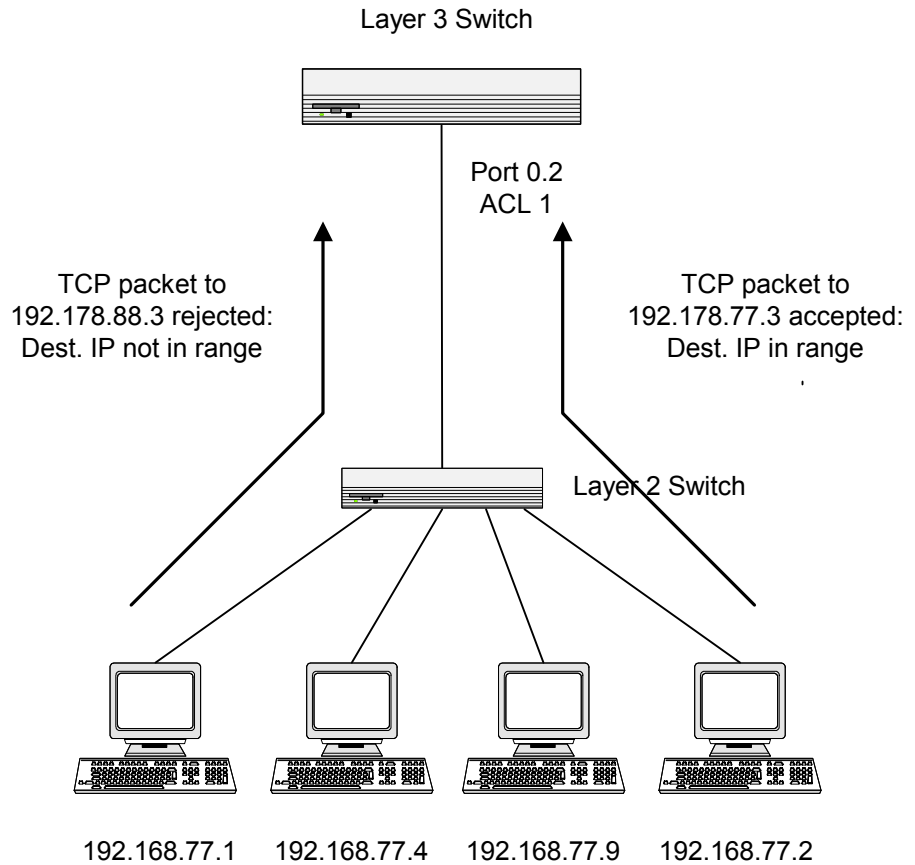


FIGURE 10. ACL example network diagram

Table 12. Example of configuring ACL support on a 7300 Series L3 Switch

ACL
<pre>Create ACL 1. config acl create 1 Create the first rule for ACL 1. config acl rule create 1 1 Define the rule: it will permit packets with a match on the specified Source IP address, after the mask has been applied, that are carrying TCP traffic, and are sent to the specified Destination IP address. config rule action 1 1 permit config rule match srcip 1 1 192.168.77.0 255.255.255.0 config rule match protocol keyword 1 1 tcp config rule match dstip 1 1 192.178.77.0 255.255.255.0 Create the second rule for ACL 1. config acl rule create 1 2 Define the rule to set similar conditions for UDP traffic as for TCP traffic. config rule action 1 2 permit config rule match dstip 1 2 192.168.77.0 255.255.255.0 config rule match protocol keyword 1 2 udp config rule match dstip 1 2 192.178.77.0 255.255.255.0 Apply the rule to inbound traffic on port 0.2. Only traffic matching the criteria will be accepted. config acl interface add 0.2 inbound 1</pre>

Use the following screens to perform the same configuration using the Graphical User Interface:

- ⦿ **QOS --> Access Control Lists --> Configuration.** To create the lists and rules.
- ⦿ **QOS --> Access Control Lists --> Rule Creation.** To define the contents of the rules.

8.0 Differentiated Services

Differentiated Services (DiffServ) is one technique for implementing Quality of Service (QoS) policies. Using DiffServ in your network allows you to directly configure the relevant parameters on the switches and routers rather than using a resource reservation protocol. This section will explain how to configure the 7300 Series Level 3 Managed Switch to identify which traffic class a packet belongs to, and how it should be handled to provide the desired quality of service. As implemented on the 7300 Series L3 Switch, DiffServ allows you to control what traffic is accepted, what traffic is transmitted, and what bandwidth guarantees are provided.

How you configure DiffServ support on a 7300 Series L3 Switch will likely vary depending on the role of the switch in your network:

-
-
- ⊙ **Edge device.** An edge device handles ingress traffic, flowing towards the core of the network, and egress traffic, flowing away from the core. An edge device will segregate inbound traffic into a small set of traffic classes, and is responsible for determining a packet's classification. Classification will be primarily based on the contents of the Layer 3 and Layer 4 headers, and will be recorded in the Differentiated Services Code Point (DSCP) added to a packet's IP header.
 - ⊙ **Interior node.** A switch in the core of the network is responsible for forwarding packets, rather than for classifying them. It will decode the DSCP code point in an incoming packet, and provide buffering and forwarding services using the appropriate queue management algorithms.

In order to configure DiffServ on a particular 7300 Series L3 Switch, you must first determine the QoS requirements for the network as a whole. The requirements are expressed in terms of rules, which are used to classify either inbound or outbound traffic on a particular interface. Rules are defined in terms of classes, policies and services:

- ⊙ **Class.** A class consists of a set of rules that identify which packets belong to the class. Inbound traffic is separated into traffic classes based on Layer 3 and 4 header data and the VLAN ID, and marked with a corresponding DSCP value. Outbound traffic is grouped into forwarding classes based on the DSCP value, and allocated priority and bandwidth accordingly. One type of class is supported:
- ⊙ **All.** Every match criterion defined for the class must be true for a match to occur.
- ⊙ **Policy.** Defines the QoS attributes for one or more traffic classes. An example of an attribute is the specification of minimum or maximum bandwidth in terms of kbps or percent of link capacity. The 7300 Series L3 Switch supports two policy types:
 - **Traffic Conditioning Policy.** This type of policy is associated with an inbound traffic class and specified the actions to be performed on packets meeting the class rules:
 - Marking the packet with a given DSCP code point
 - Policing packets by dropping or re-marking those that exceed the class's assigned data rate
 - Counting the traffic within the class
 - **Service Provisioning Policy.** This type of policy is associated with an outbound traffic class and affects how packets are transmitted
- ⊙ **Service.** Assigns a policy to an interface for either inbound or outbound traffic

8.1 Differentiated Services Configuration Example

This example shows how a network administrator can provide equal access to the Internet (or other external network) to different departments within a company. Each of four departments has its own VLAN, and each VLAN is allocated 25% of the available bandwidth on the port accessing the Internet.

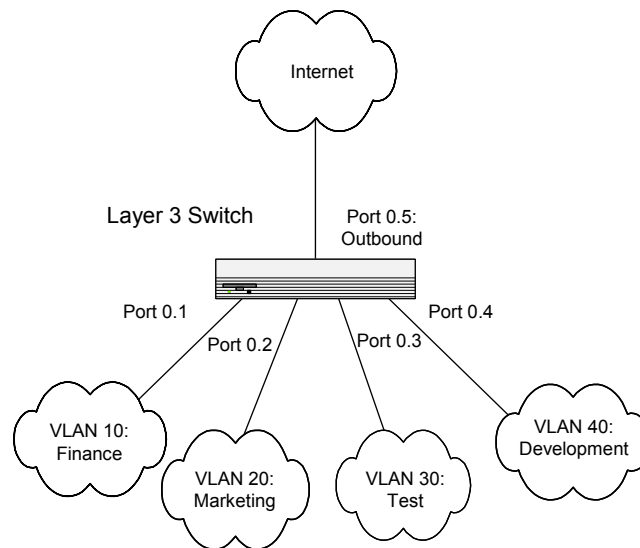


FIGURE 11. DiffServ Internet access example network diagram

Table 13. Example of configuring DiffServ on a 7300 Series L3 Switch

DiffServ inbound configuration
<pre> Create a DiffServ class of type "all" for each of the departments, and name them. config diffserv class create all class_vlan10 config diffserv class create all class_vlan20 config diffserv class create all class_vlan30 config diffserv class create all class_vlan40 Define the match criteria -- VLAN ID -- for the new classes. config diffserv class match vlan class_vlan10 10 config diffserv class match vlan class_vlan20 20 config diffserv class match vlan class_vlan30 30 config diffserv class match vlan class_vlan40 40 Create and name a conditioning policy for inbound traffic, then add the previously created classes to the new policy. config diffserv policy create pol_vlan in config diffserv policy class add pol_vlan class_vlan10 config diffserv policy class add pol_vlan class_vlan20 config diffserv policy class add pol_vlan class_vlan30 config diffserv policy class add pol_vlan class_vlan40 Define the action -- mark -- for each class and policy. config diffserv policy mark ipdscp pol_vlan class_vlan10 cs1 config diffserv policy mark ipdscp pol_vlan class_vlan20 cs2 config diffserv policy mark ipdscp pol_vlan class_vlan30 cs3 config diffserv policy mark ipdscp pol_vlan class_vlan40 cs4 Attach the defined policy to the inbound interfaces. config diffserv service add in 0.1 pol_vlan config diffserv service add in 0.2 pol_vlan config diffserv service add in 0.3 pol_vlan config diffserv service add in 0.4 pol_vlan </pre>

DiffServ outbound configuration

Activate DiffServ for the switch.

```
config diffserv adminmode enable
```

Create and name a DiffServ class of type "all" for the four outbound classes.

```
config diffserv class create all class_finance
config diffserv class create all class_marketing
config diffserv class create all class_test
config diffserv class create all class_development
```

Define the match criteria for the new classes.

```
config diffserv class match ipdscp class_finance cs1
config diffserv class match ipdscp class_marketing cs2
config diffserv class match ipdscp class_test cs3
config diffserv class match ipdscp class_development cs4
```

Create a DiffServ policy for the outbound traffic and give it a name, then add the previously created classes.

```
config diffserv policy create pol_share out
config diffserv policy class add pol_share class_finance
config diffserv policy class add pol_share class_marketing
config diffserv policy class add pol_share class_test
config diffserv policy class add pol_share class_development
```

Define the bandwidth to be reserved for the classes as a percentage of total link capacity.

```
config diffserv policy bandwidth percent pol_share class_finance
25
config diffserv policy bandwidth percent pol_share
class_marketing 25
config diffserv policy bandwidth percent pol_share class_test 25
config diffserv policy bandwidth percent pol_share
class_development 25
```

Attach the defined policy to the outbound interface.

```
config diffserv service add out 0.5 pol_share
```

Use the following screens to perform the same configuration using the Graphical User Interface:

- ⊙ **QOS --> Differentiated Services --> Diffserv Configuration.** To activate Diffserv.
- ⊙ **QOS --> Differentiated Services --> Class Creation.** To create the classes.
- ⊙ **QOS --> Differentiated Services --> Policy Configuration.** To create the policies.
- ⊙ **QOS --> Differentiated Services --> Policy Class Definition.** To define the policies.
- ⊙ **QOS --> Differentiated Services--> Service Configuration.** To attach the policy to an interface.

8.2 Differentiated Services for Voice Over IP Configuration Example

One of the most valuable uses of DiffServ is to support Voice over IP (VoIP). VoIP traffic is inherently time-sensitive: for a network to provide acceptable service, a guaran-

teed transmission rate is vital. This example shows one way to provide the necessary quality of service: how to set up a class for UDP traffic, have that traffic marked on the inbound side, and then expedite the traffic on the outbound side. The configuration script is for Router 1 in the accompanying diagram: a similar script should be applied to Router 2.

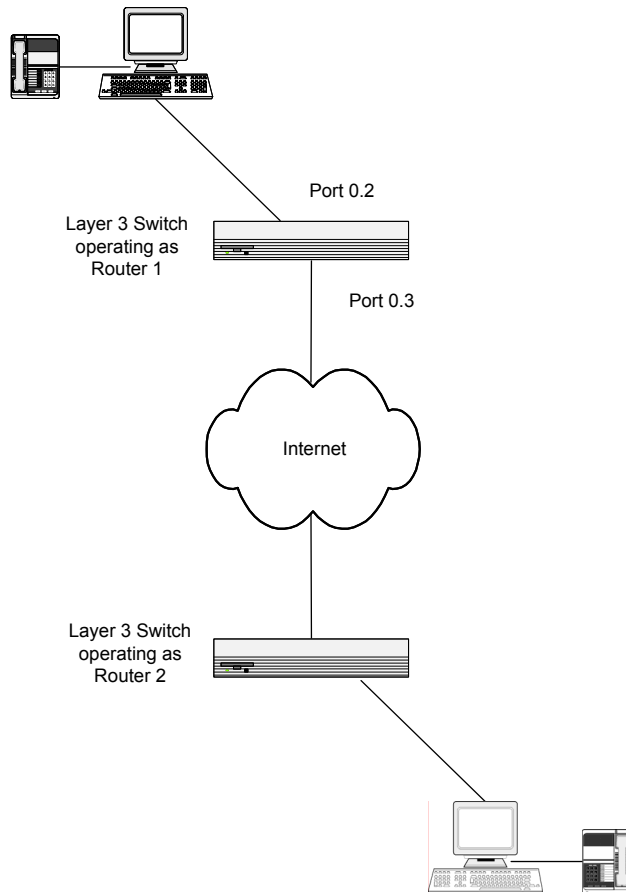


FIGURE 12. DiffServ VoIP example network diagram

Table 14. Example of configuring DiffServ VoIP support on a 7300 Series L3 Switch configuration

DiffServ
<p><i>Activate DiffServ for the switch.</i> config diffserv adminmode enable</p> <p><i>Create a DiffServ class of type "all" and give it a name.</i> config diffserv class create all class_voip</p> <p><i>Define the match criteria for the new class</i> config diffserv class match protocol keyword class_voip udp</p> <p><i>Create a DiffServ policy for inbound traffic and give it a name, then add the previously created class to the new policy.</i> config diffserv policy create pol_3 in config diffserv policy class add pol_3 class_voip</p> <p><i>Define the policy. Conforming traffic will be marked.</i> config diffserv policy mark ipdscp pol_3 class_voip ef</p> <p><i>Create a second class, and define its match criteria to be a DSCP value of ef.</i> config diffserv class create all class_ef config diffserv class match ipdscp class_ef ef</p> <p><i>Create and attach the policy for outbound traffic.</i> config diffserv policy create pol_4 out config diffserv policy class add pol_4 class_ef</p> <p><i>Attach the defined policies to interfaces.</i> config diffserv service add in 0.2 pol_3 config diffserv service add out 0.3 pol_4</p>