Module 5: STP Concepts

Instructor Materials

Switching, Routing and Wireless Essentials v7.0 (SRWE)

Module Objectives

Module Title: STP Concepts

Module Objective: Explain how STP enables redundancy in a Layer 2 network.

Topic Title	Topic Objective
Purpose of STP	Explain common problems in a redundant, L2 switched network.
STP Operations	Explain how STP operates in a simple switched network.
Evolution of STP	Explain how Rapid PVST+ operates.

5.1 Purpose of STP

Purpose of STP

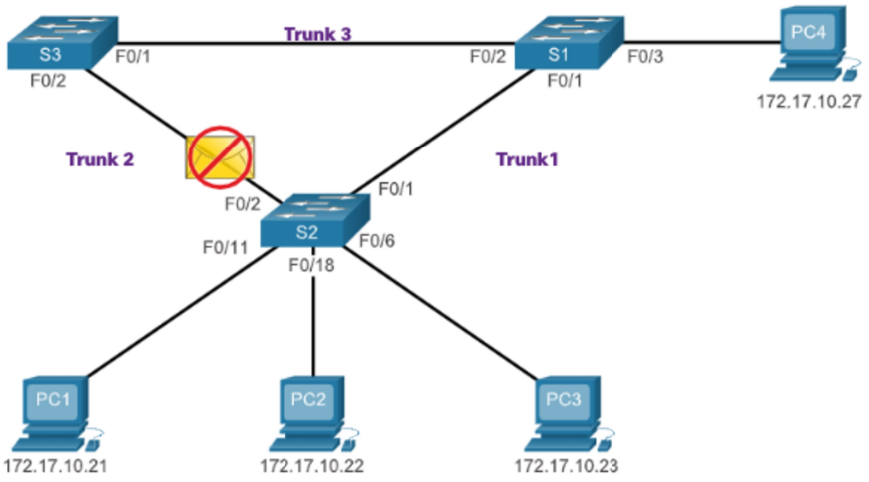
Redundancy in Layer 2 Switched Networks

- This topic covers the causes of loops in a Layer 2 network and briefly explains how spanning tree protocol works. Redundancy is an important part of the hierarchical design for eliminating single points of failure and preventing disruption of network services to users. Redundant networks require the addition of physical paths, but logical redundancy must also be part of the design. Having alternate physical paths for data to traverse the network makes it possible for users to access network resources, despite path disruption. However, redundant paths in a switched Ethernet network may cause both physical and logical Layer 2 loops.
- Ethernet LANs require a loop-free topology with a single path between any two devices. A loop in an Ethernet LAN can cause continued propagation of Ethernet frames until a link is disrupted and breaks the loop.

Purpose of STP

Spanning Tree Protocol

- Spanning Tree Protocol (STP) is a loop-prevention network protocol that allows for redundancy while creating a loop-free Layer 2 topology.
- STP logically blocks physical loops in a Layer 2 network, preventing frames from circling the network forever.

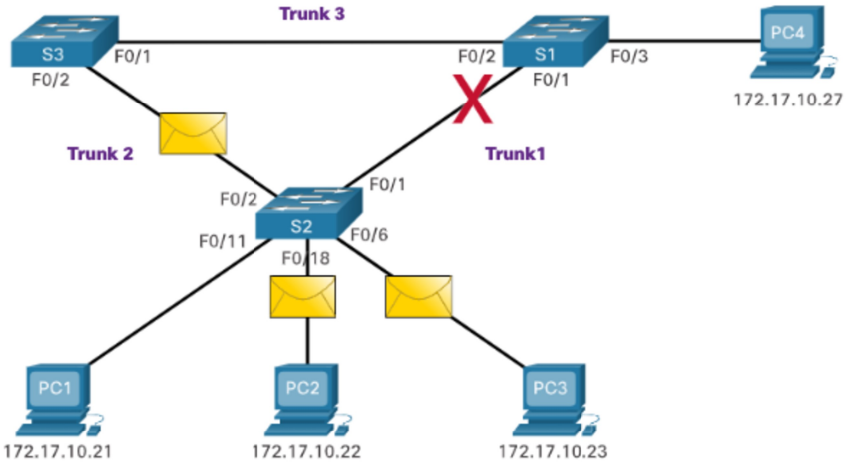


S2 drops the frame because it received it on a blocked port.

Purpose of STP

STP Recalculation

STP compensates for a failure in the network by recalculating and opening up previously blocked ports.



Purpose of STP

Issues with Redundant Switch Links

- Path redundancy provides multiple network services by eliminating the possibility of a single point of failure. When multiple paths exist between two devices on an Ethernet network, and there is no spanning tree implementation on the switches, a Layer 2 loop occurs. A Layer 2 loop can result in MAC address table instability, link saturation, and high CPU utilization on switches and end-devices, resulting in the network becoming unusable.
- Layer 2 Ethernet does not include a mechanism to recognize and eliminate endlessly looping frames. Both IPv4 and IPv6 include a mechanism that limits the number of times a Layer 3 networking device can retransmit a packet. A router will decrement the TTL (Time to Live) in every IPv4 packet, and the Hop Limit field in every IPv6 packet. When these fields are decremented to 0, a router will drop the packet. Ethernet and Ethernet switches have no comparable mechanism for limiting the number of times a switch retransmits a Layer 2 frame. STP was developed specifically as a loop prevention mechanism for Layer 2 Ethernet.

Purpose of STP

Layer 2 Loops

- Without STP enabled, Layer 2 loops can form, causing broadcast, multicast and unknown unicast frames to loop endlessly. This can bring down a network quickly.
- When a loop occurs, the MAC address table on a switch will constantly change with the updates from the broadcast frames, which results in MAC database instability. This can cause high CPU utilization, which makes the switch unable to forward frames.
- An unknown unicast frame is when the switch does not have the destination MAC address in its MAC address table and must forward the frame out all ports, except the ingress port.

Purpose of STP

Broadcast Storm

- A broadcast storm is an abnormally high number of broadcasts overwhelming the network during a specific amount of time. Broadcast storms can disable a network within seconds by overwhelming switches and end devices. Broadcast storms can be caused by a hardware problem such as a faulty NIC or from a Layer 2 loop in the network.
- Layer 2 broadcasts in a network, such as ARP Requests are very common. Layer 2 multicasts are typically forwarded the same way as a broadcast by the switch. IPv6 packets are never forwarded as a Layer 2 broadcast, ICMPv6 Neighbor Discovery uses Layer 2 multicasts.
- A host caught in a Layer 2 loop is not accessible to other hosts on the network. Additionally, due to the constant changes in its MAC address table, the switch does not know out of which port to forward unicast frames.
- To prevent these issues from occurring in a redundant network, some type of spanning tree must be enabled on the switches. Spanning tree is enabled, by default, on Cisco switches to prevent Layer 2 loops from occurring.

Purpose of STP

The Spanning Tree Algorithm

- STP is based on an algorithm invented by Radia Perlman while working for Digital Equipment Corporation, and published in the 1985 paper "An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN." Her spanning tree algorithm (STA) creates a loop-free topology by selecting a single root bridge where all other switches determine a single least-cost path.
- STP prevents loops from occurring by configuring a loop-free path through the network using strategically placed "blocking-state" ports. The switches running STP are able to compensate for failures by dynamically unblocking the previously blocked ports and permitting traffic to traverse the alternate paths.

Purpose of STP

The Spanning Tree Algorithm (Cont.)

How does the STA create a loop-free topology?

- Selecting a Root Bridge: This bridge (switch) is the reference point for the entire network to build a spanning tree around.
- Block Redundant Paths: STP ensures that there is only one logical path between all destinations on the network by intentionally blocking redundant paths that could cause a loop. When a port is blocked, user data is prevented from entering or leaving that port.
- Create a Loop-Free Topology: A blocked port has the effect of making that link a non-forwarding link between the two switches. This creates a topology where each switch has only a single path to the root bridge, similar to branches on a tree that connect to the root of the tree.
- Recalculate in case of Link Failure: The physical paths still exist to provide redundancy, but these paths are disabled to prevent the loops from occurring. If the path is ever needed to compensate for a network cable or switch failure, STP recalculates the paths and unblocks the necessary ports to allow the redundant path to become active. STP recalculations can also occur any time a new switch or new inter-switch link is added to the network.

Purpose of STP

Video – Observe STP Operation

This video demonstrates the use of STP in a network environment.

Packet Tracer – Investigate STP Loop Prevention

In this Packet Tracer activity, you will complete the following objectives:

- Create and configure a simple three switch network with STP.
- View STP operation.
- Disable STP and view operation again.

5.2 STP Operations

STP Operations

Steps to a Loop-Free Topology

Using the STA, STP builds a loop-free topology in a four-step process:

1. Elect the root bridge.
2. Elect the root ports.
3. Elect designated ports.
4. Elect alternate (blocked) ports.

- During STA and STP functions, switches use Bridge Protocol Data Units (BPDUs) to share information about themselves and their connections. BPDUs are used to elect the root bridge, root ports, designated ports, and alternate ports.
- Each BPDU contains a bridge ID (BID) that identifies which switch sent the BPDU. The BID is involved in making many of the STA decisions including root bridge and port roles.
- The BID contains a priority value, the MAC address of the switch, and an extended system ID. The lowest BID value is determined by the combination of these three fields.

STP Operations

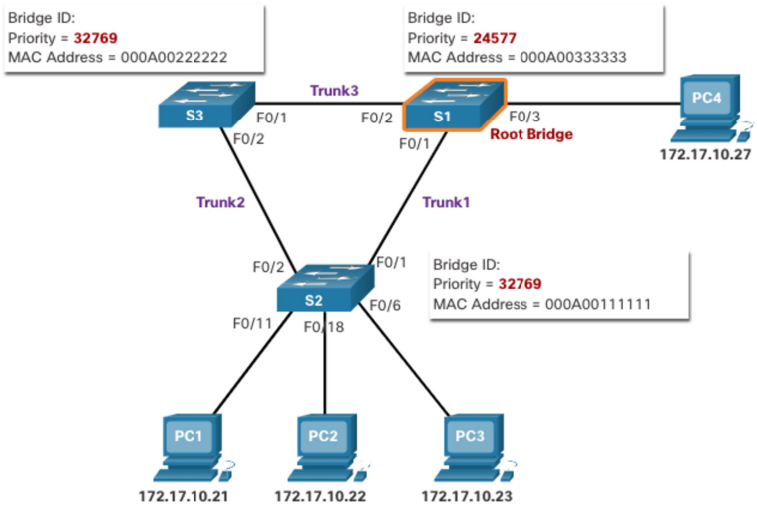
Steps to a Loop-Free Topology (Cont.)

- **Bridge Priority:** The default priority value for all Cisco switches is the decimal value 32768. The range is 0 to 61440 in increments of 4096. A lower bridge priority is preferable. A bridge priority of 0 takes precedence over all other bridge priorities.
- **Extended System ID:** The extended system ID value is a decimal value added to the bridge priority value in the BID to identify the VLAN for this BPDU.
- **MAC address:** When two switches are configured with the same priority and have the same extended system ID, the switch having the MAC address with the lowest value, expressed in hexadecimal, will have the lower BID.

STP Operations

1. Elect the Root Bridge

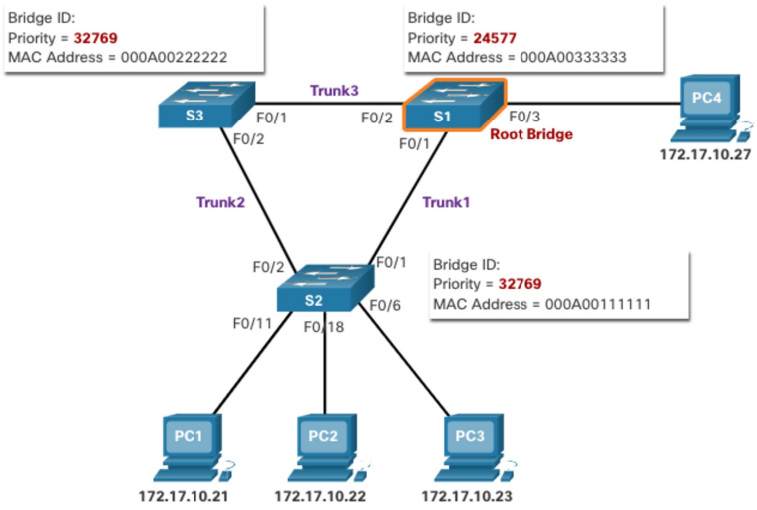
- The STA designates a single switch as the root bridge and uses it as the reference point for all path calculations. Switches exchange BPDUs to build the loop-free topology beginning with selecting the root bridge.
- All switches in the broadcast domain participate in the election process. After a switch boots, it begins to send out BPDU frames every two seconds. These BPDU frames contain the BID of the sending switch and the BID of the root bridge, known as the Root ID.
- The switch with the lowest BID will become the root bridge. At first, all switches declare themselves as the root bridge with their own BID set as the Root ID. Eventually, the switches learn through the exchange of BPDUs which switch has the lowest BID and will agree on one root bridge.



STP Operations

Impact of Default BIDs

- Because the default BID is 32768, it is possible for two or more switches to have the same priority. In this scenario, where the priorities are the same, the switch with the lowest MAC address will become the root bridge. The administrator should configure the desired root bridge switch with a lower priority.
- In the figure, all switches are configured with the same priority of 32769. Here the MAC address becomes the deciding factor as to which switch becomes the root bridge. The switch with the lowest hexadecimal MAC address value is the preferred root bridge. In this example, S2 has the lowest value for its MAC address and is elected as the root bridge for that spanning tree instance.
- **Note**: The priority of all the switches is 32769. The value is based on the 32768 default bridge priority and the extended system ID (VLAN 1 assignment) associated with each switch (32768+1).



STP Operations

Determine the Root Path Cost

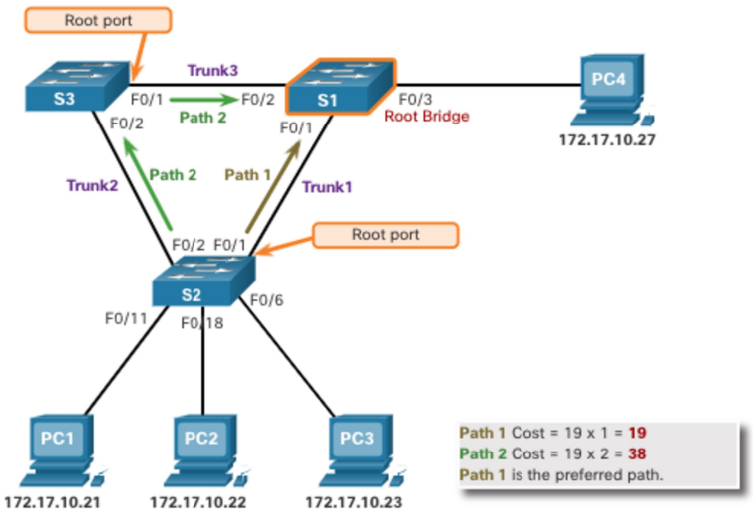
- When the root bridge has been elected for a given spanning tree instance, the STA starts determining the best paths to the root bridge from all destinations in the broadcast domain. The path information, known as the internal root path cost, is determined by the sum of all the individual port costs along the path from the switch to the root bridge.
- When a switch receives the BPDU, it adds the ingress port cost of the segment to determine its internal root path cost.
- The default port costs are defined by the speed at which the port operates. The table shows the default port costs suggested by IEEE. Cisco switches by default use the values as defined by the IEEE 802.1D standard, also known as the short path cost, for both STP and RSTP.
- Although switch ports have a default port cost associated with them, the port cost is configurable. The ability to configure individual port costs gives the administrator the flexibility to manually control the spanning tree paths to the root bridge.

Link Speed	STP Cost: IEEE 802.1D-1998	RSTP Cost: IEEE 802.1w-2004
10 Gbps	2	2,000
1 Gbps	4	20,000
100 Mbps	19	200,000
10 Mbps	100	2,000,000

STP Operations

2. Elect the Root Ports

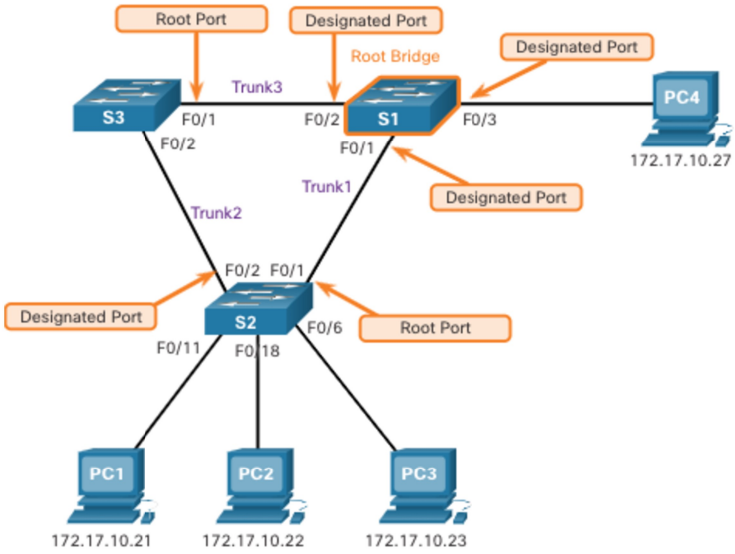
- After the root bridge has been determined, the STA algorithm is used to select the root port. Every non-root switch will select one root port. The root port is the port closest to the root bridge in terms of overall cost to the root bridge. This overall cost is known as the internal root path cost.
- The internal root path cost is equal to the sum of all the port costs along the path to the root bridge, as shown in the figure. Paths with the lowest cost become preferred, and all other redundant paths are blocked. In the example, the internal root path cost from S2 to the root bridge S1 over path 1 is 19 while the internal root path cost over path 2 is 38. Because path 1 has a lower overall path cost to the root bridge, it is the preferred path and F0/1 becomes the root port on S2.



STP Operations

3. Elect Designated Ports

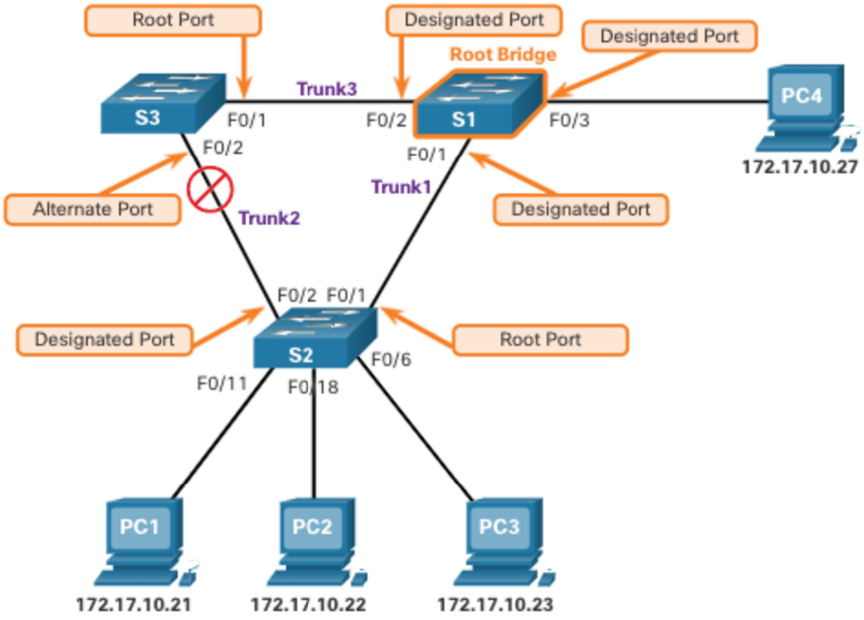
- Every segment between two switches will have one designated port. The designated port is a port on the segment that has the internal root path cost to the root bridge. In other words, the designated port has the best path to receive traffic leading to the root bridge.
- What is not a root port or a designated port becomes an alternate or blocked port.
- All ports on the root bridge are designated ports.
- If one end of a segment is a root port, the other end is a designated port.
- All ports attached to end devices are designated ports.
- On segments between two switches where neither of the switches is the root bridge, the port on the switch with the least-cost path to the root bridge is a designated port.



STP Operations

4. Elect Alternate (Blocked) Ports

If a port is not a root port or a designated port, then it becomes an alternate (or backup) port. Alternate ports are in discarding or blocking state to prevent loops. In the figure, the STA has configured port F0/2 on S3 in the alternate role. Port F0/2 on S3 is in the blocking state and will not forward Ethernet frames. All other inter-switch ports are in forwarding state. This is the loop-prevention part of STP.



STP Operations

Elect a Root Port from Multiple Equal-Cost Paths

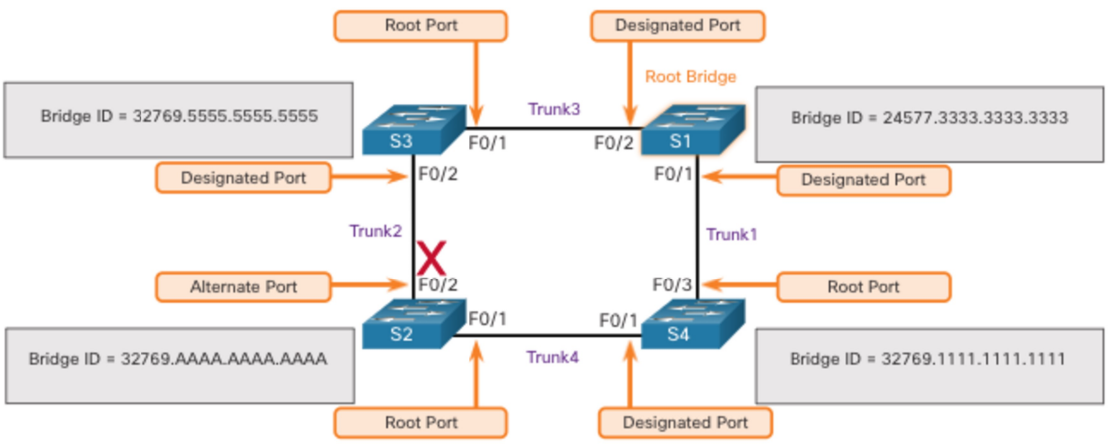
When a switch has multiple equal-cost paths to the root bridge, the switch will determine a port using the following criteria:

- Lowest sender BID
- Lowest sender port priority
- Lowest sender port ID

STP Operations

Elect a Root Port from Multiple Equal-Cost Paths (Cont.)

Lowest Sender BID: This topology has four switches with switch S1 as the root bridge. Port F0/1 on switch S3 and port F0/3 on switch S4 have been selected as root ports because they have the root path cost to the root bridge for their respective switches. S2 has two ports, F0/1 and F0/2 with equal cost paths to the root bridge. The bridge IDs of S3 and S4, will be used to break the tie. This is known as the sender's BID. S3 has a BID of 32769.5555.5555.5555 and S4 has a BID of 32769.1111.1111.1111. Because S4 has a lower BID, the F0/1 port of S2, which is the port connected to S4, will be the root port.

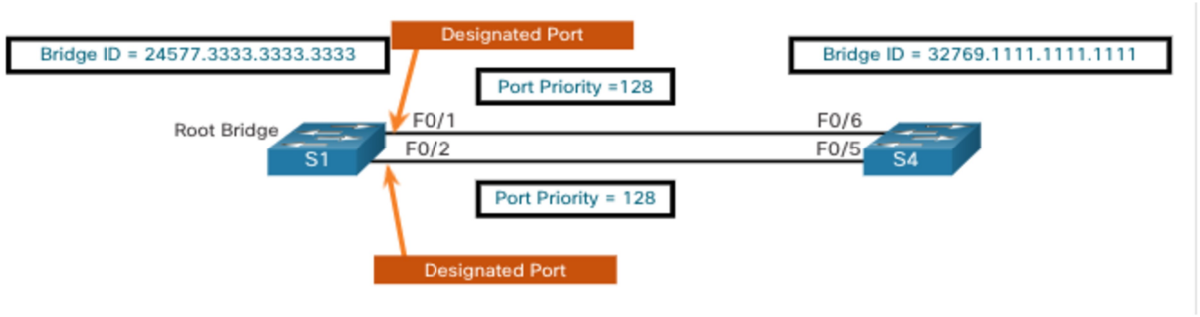


STP Operations

Elect a Root Port from Multiple Equal-Cost Paths (Cont.)

Lowest Sender Port Priority: This topology has two switches which are connected with two equal-cost paths between them. S1 is the root bridge, so both of its ports are designated ports.

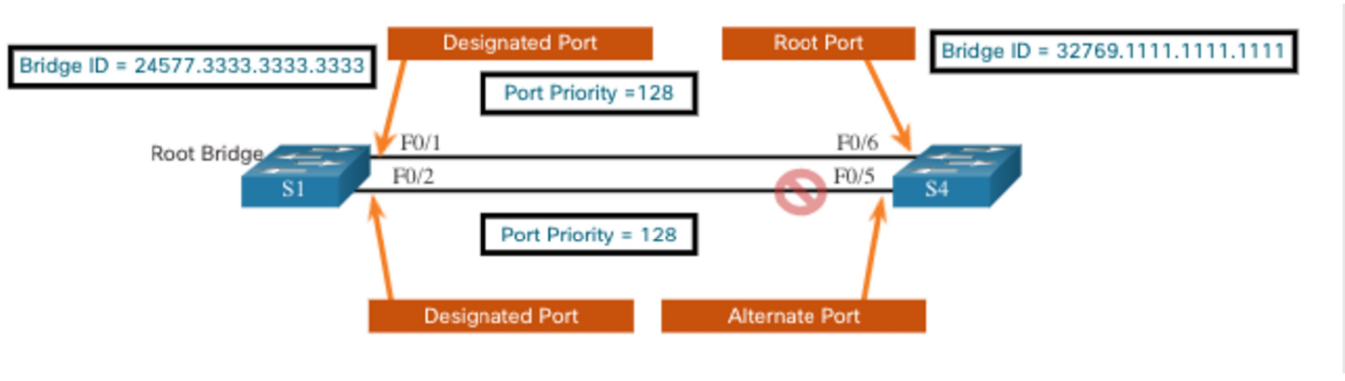
- S4 has two ports with equal-cost paths to the root bridge. Because both ports are connected to the same switch, the sender's BID (S1) is equal. So the first step is a tie.
- Next, is the sender's (S1) port priority. The default port priority is 128, so both ports on S1 have the same port priority. This is also a tie. However, if either port on S1 was configured with a lower port priority, S4 would put its adjacent port in forwarding state. The other port on S4 would be a blocking state.



STP Operations

Elect a Root Port from Multiple Equal-Cost Paths (Cont.)

- **Lowest Sender Port ID:** The last tie-breaker is the lowest sender's port ID. Switch S4 has received BPDUs from port F0/1 and port F0/2 on S1. The decision is based on the sender's port ID, not the receiver's port ID. Because the port ID of F0/1 on S1 is lower than port F0/2, the port F0/6 on switch S4 will be the root port. This is the port on S4 that is connected to the F0/1 port on S1.
- Port F0/5 on S4 will become an alternate port and placed in the blocking state.



STP Operations

STP Timers and Port States

STP convergence requires three timers, as follows:

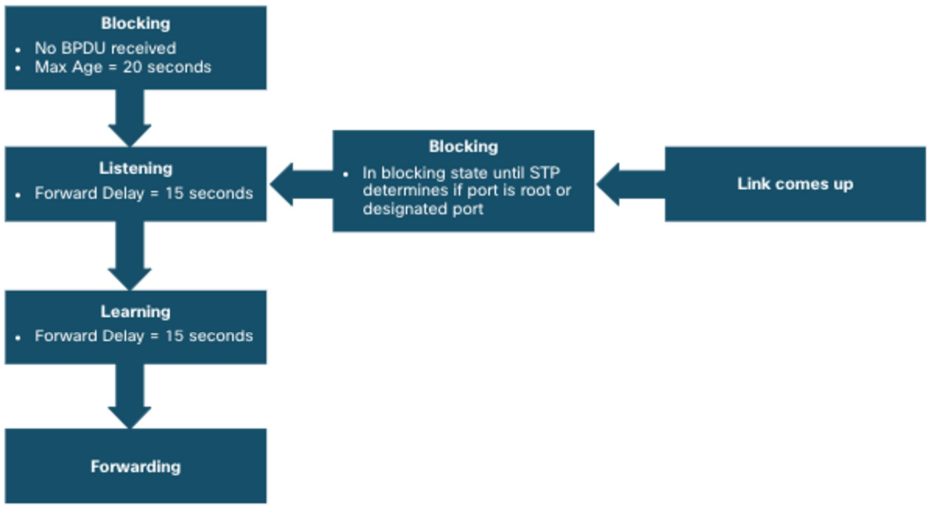
- **Hello Timer** -The hello time is the interval between BPDUs. The default is 2 seconds but can be modified to between 1 and 10 seconds.
- **Forward Delay Timer** -The forward delay is the time that is spent in the listening and learning state. The default is 15 seconds but can be modified to between 4 and 30 seconds.
- **Max Age Timer** -The max age is the maximum length of time that a switch waits before attempting to change the STP topology. The default is 20 seconds but can be modified to between 6 and 40 seconds.

Note: The default times can be changed on the root bridge, which dictates the value of these timers for the STP domain.

STP Operations

STP Timers and Port States (Cont.)

STP facilitates the logical loop-free path throughout the broadcast domain. The spanning tree is determined through the information learned by the exchange of the BPDU frames between the interconnected switches. If a switch port transitions directly from the blocking state to the forwarding state without information about the full topology during the transition, the port can temporarily create a data loop. For this reason, STP has five ports states, four of which are operational port states as shown in the figure. The disabled state is considered non-operational.



STP Operations

Operational Details of Each Port State

The table summarizes the operational details of each port state

Port State	BPDU	MAC Address Table	Forwarding Data Frames
Blocking	Receive only	No update	No
Listening	Receive and send	No update	No
Learning	Receive and send	Updating table	No
Forwarding	Receive and send	Updating table	Yes
Disabled	None sent or received	No update	No

STP Operations

Per-VLAN Spanning Tree

STP can be configured to operate in an environment with multiple VLANs. In Per-VLAN Spanning Tree (PVST) versions of STP, there is a root bridge elected for each spanning tree instance. This makes it possible to have different root bridges for different sets of VLANs. STP operates a separate instance of STP for each individual VLAN. If all ports on all switches are members of VLAN 1, then there is only one spanning tree instance.

5.3 Evolution of STP

Evolution of STP

Different Versions of STP

- Many professionals generically use spanning tree and STP to refer to the various implementations of spanning tree, such as Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP). In order to communicate spanning tree concepts correctly, it is important to refer to the implementation or standard of spanning tree in context.
- The latest IEEE documentation on spanning tree (IEEE-802-1D-2004) says, "STP has now been superseded by the Rapid Spanning Tree Protocol (RSTP)."The IEEE uses "STP" to refer to the original implementation of spanning tree and "RSTP" to describe the version of spanning tree specified in IEEE-802.1D-2004.
- Because the two protocols share much of the same terminology and methods for the loop-free path, the primary focus will be on the current standard and the Cisco proprietary implementations of STP and RSTP.
- Cisco switches running IOS 15.0 or later, run PVST+ by default. This version incorporates many of the specifications of IEEE 802.1D-2004, such as alternate ports in place of the former non-designated ports. Switches must be explicitly configured for rapid spanning tree mode in order to run the rapid spanning tree protocol.

Evolution of STP

Different Versions of STP (Cont.)

STP Variety	Description
STP	This is the original IEEE 802.1D version (802.1D-1998 and earlier) that provides a loop-free topology in a network with redundant links. Also called Common Spanning Tree (CST), it assumes one spanning tree instance for the entire bridged network, regardless of the number of VLANs.
PVST+	Per-VLAN Spanning Tree (PVST+) is a Cisco enhancement of STP that provides a separate 802.1D spanning tree instance for each VLAN configured in the network. PVST+ supports PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard, and loop guard.
802.1D-2004	This is an updated version of the STP standard, incorporating IEEE 802.1w.
RSTP	Rapid Spanning Tree Protocol (RSTP) or IEEE 802.1w is an evolution of STP that provides faster convergence than STP.
Rapid PVST+	This is a Cisco enhancement of RSTP that uses PVST+ and provides a separate instance of 802.1w per VLAN. Each separate instance supports PortFast, BPDU guard, BPDU filter, root guard, and loop guard.
MSTP	Multiple Spanning Tree Protocol (MSTP) is an IEEE standard inspired by the earlier Cisco proprietary Multiple Instance STP (MISTP) implementation. MSTP maps multiple VLANs into the same spanning tree instance.
MST	Multiple Spanning Tree (MST) is the Cisco implementation of MSTP, which provides up to 16 instances of RSTP and combines many VLANs with the same physical and logical topology into a common RSTP instance. Each instance supports PortFast, BPDU guard, BPDU filter, root guard, and loop guard.

Evolution of STP

RSTP Concepts

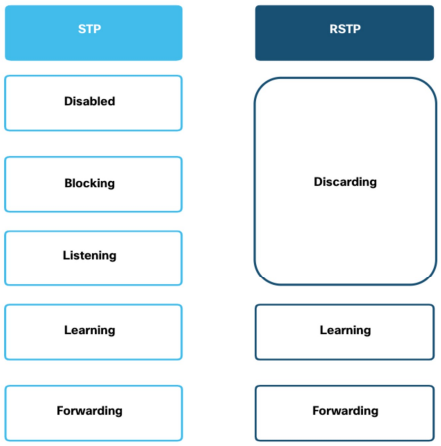
- RSTP (IEEE 802.1w) supersedes the original 802.1D while retaining backward compatibility. The 802.1w STP terminology remains primarily the same as the original IEEE 802.1D STP terminology. Most parameters have been left unchanged. Users that are familiar with the original STP standard can easily configure RSTP. The same spanning tree algorithm is used for both STP and RSTP to determine port roles and topology.
- RSTP increases the speed of the recalculation of the spanning tree when the Layer 2 network topology changes. RSTP can achieve much faster convergence in a properly configured network, sometimes in as little as a few hundred milliseconds. If a port is configured to be an alternate port it can immediately change to a forwarding state without waiting for the network to converge.

Note: Rapid PVST+ is the Cisco implementation of RSTP on a per-VLAN basis. With Rapid PVST+ an independent instance of RSTP runs for each VLAN.

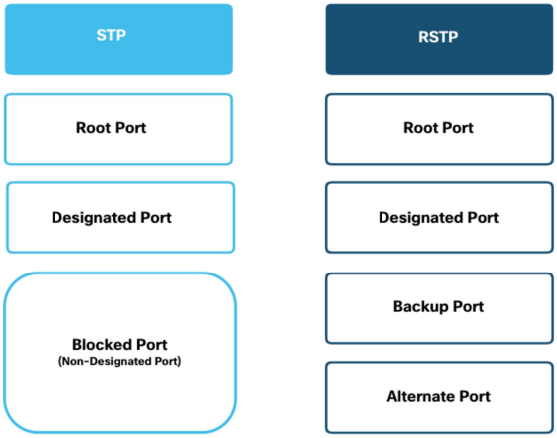
Evolution of STP

RSTP Port States and Port Roles

There are only three port states in RSTP that correspond to the three possible operational states in STP. The 802.1D disabled, blocking, and listening states are merged into a unique 802.1w discarding state.



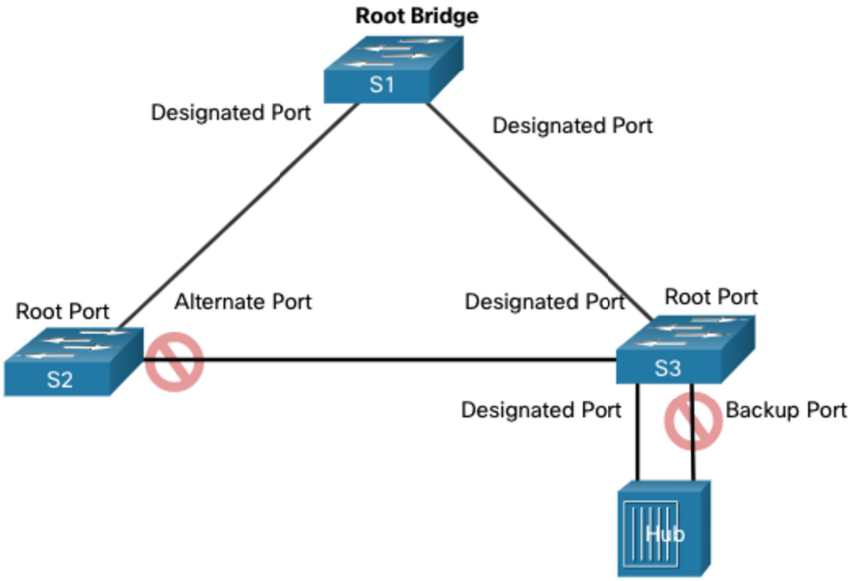
Root ports and designated ports are the same for both STP and RSTP. However, there are two RSTP port roles that correspond to the blocking state of STP. In STP, a blocked port is defined as not being the designated or root port. RSTP has two port roles for this purpose.



Evolution of STP

RSTP Port States and Port Roles (Cont.)

The alternate port has an alternate path to the root bridge. The backup port is a backup to a shared medium, such as a hub. A backup port is less common because hubs are now considered legacy devices.



Evolution of STP

PortFast and BPDU Guard

- When a device is connected to a switch port or when a switch powers up, the switch port goes through both the listening and learning states, each time waiting for the Forward Delay timer to expire. This delay is 15 seconds for each state for a total of 30 seconds. This can present a problem for DHCP clients trying to discover a DHCP server because the DHCP process may timeout. The result is that an IPv4 client will not receive a valid IPv4 address.
- When a switch port is configured with PortFast, that port transitions from blocking to forwarding state immediately, avoiding the 30 second delay. You can use PortFast on access ports to allow devices connected to these ports to access the network immediately. PortFast should only be used on access ports. If you enable PortFast on a port connecting to another switch, you risk creating a spanning tree loop.
- A PortFast-enabled switch port should never receive BPDUs because that would indicate that switch is connected to the port, potentially causing a spanning tree loop. Cisco switches support a feature called BPDU guard. When enabled, it immediately puts the switch port in an errdisabled (error-disabled) state upon receipt of any BPDU. This protects against potential loops by effectively shutting down the port. The administrator must manually put the interface back into service.

Evolution of STP

Alternatives to STP

- Over the years, organizations required greater resiliency and availability in the LAN. Ethernet LANs went from a few interconnected switches connected to a single router, to a sophisticated hierarchical network design including access, distribution and core layer switches.
- Depending on the implementation, Layer 2 may include not only the access layer, but also the distribution or even the core layers. These designs may include hundreds of switches, with hundreds or even thousands of VLANs. STP has adapted to the added redundancy and complexity with enhancements, as part of RSTP and MSTP.
- An important aspect to network design is fast and predictable convergence when there is a failure or change in the topology. Spanning tree does not offer the same efficiencies and predictabilities provided by routing protocols at Layer 3.
- Layer 3 routing allows for redundant paths and loops in the topology, without blocking ports. For this reason, some environments are transitioning to Layer 3 everywhere except where devices connect to the access layer switch. In other words, the connections between access layer switches and distribution switches would be Layer 3 instead of Layer 2.

Module 6: EtherChannel

Instructor Materials

Switching, Routing and Wireless Essentials v7.0 (SRWE)

Module Objectives

Module Title: EtherChannel

Module Objective: Troubleshoot EtherChannel on switched links.

Topic Title	Topic Objective
EtherChannel Operation	Describe EtherChannel technology.
Configure EtherChannel	Configure EtherChannel.
Verify and Troubleshoot EtherChannel	Troubleshoot EtherChannel.

6.1 EtherChannel Operation

EtherChannel Operation
Link Aggregation

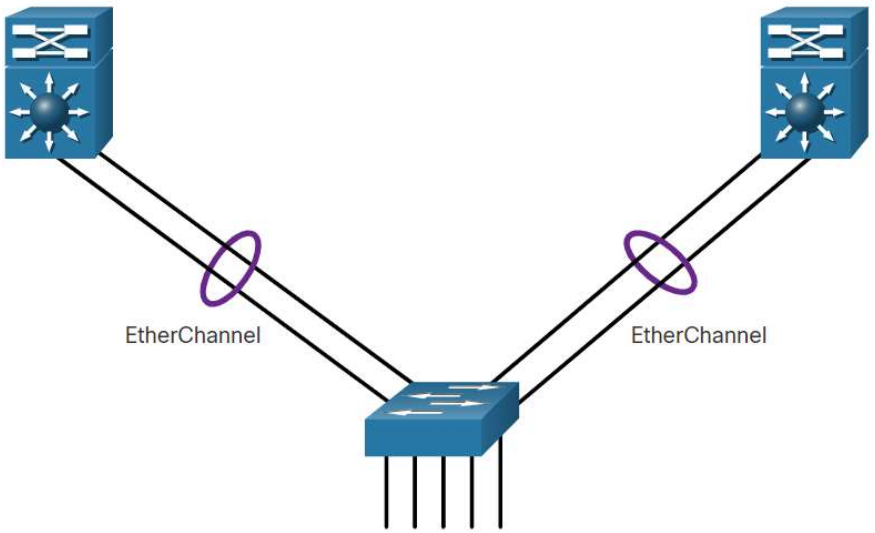
- There are scenarios in which more bandwidth or redundancy between devices is needed than what can be provided by a single link. Multiple links could be connected between devices to increase bandwidth. However, Spanning Tree Protocol (STP), which is enabled on Layer 2 devices like Cisco switches by default, will block redundant links to prevent switching loops.
- A link aggregation technology is needed that allows redundant links between devices that will not be blocked by STP. That technology is known as EtherChannel.
- EtherChannel is a link aggregation technology that groups multiple physical Ethernet links together into one single logical link. It is used to provide fault-tolerance, load sharing, increased bandwidth, and redundancy between switches, routers, and servers.
- EtherChannel technology makes it possible to combine the number of physical links between the switches to increase the overall speed of switch-to-switch communication.

EtherChannel Operation

EtherChannel

EtherChannel technology was originally developed by Cisco as a LAN switch-to-switch technique of grouping several Fast Ethernet or Gigabit Ethernet ports into one logical channel.

When an EtherChannel is configured, the resulting virtual interface is called a port channel. The physical interfaces are bundled together into a port channel interface, as shown in the figure.



EtherChannel Operation

Advantages of EtherChannel

EtherChannel technology has many advantages, including the following:

- Most configuration tasks can be done on the EtherChannel interface instead of on each individual port, ensuring configuration consistency throughout the links.
- EtherChannel relies on existing switch ports. There is no need to upgrade the link to a faster and more expensive connection to have more bandwidth.
- Load balancing takes place between links that are part of the same EtherChannel.
- EtherChannel creates an aggregation that is seen as one logical link. When several EtherChannel bundles exist between two switches, STP may block one of the bundles to prevent switching loops. When STP blocks one of the redundant links, it blocks the entire EtherChannel. This blocks all the ports belonging to that EtherChannel link. Where there is only one EtherChannel link, all physical links in the EtherChannel are active because STP sees only one (logical) link.
- EtherChannel provides redundancy because the overall link is seen as one logical connection. Additionally, the loss of one physical link within the channel does not create a change in the topology.

EtherChannel Operation

Implementation Restrictions

EtherChannel has certain implementation restrictions, including the following:

- Interface types cannot be mixed. For example, Fast Ethernet and Gigabit Ethernet cannot be mixed within a single EtherChannel.
- Currently each EtherChannel can consist of up to eight compatibly-configured Ethernet ports. EtherChannel provides full-duplex bandwidth up to 800 Mbps (Fast EtherChannel) or 8 Gbps (Gigabit EtherChannel) between one switch and another switch or host.
- The Cisco Catalyst 2960 Layer 2 switch currently supports up to six EtherChannels.
- The individual EtherChannel group member port configuration must be consistent on both devices. If the physical ports of one side are configured as trunks, the physical ports of the other side must also be configured as trunks within the same native VLAN. Additionally, all ports in each EtherChannel link must be configured as Layer 2 ports.
- Each EtherChannel has a logical port channel interface. A configuration applied to the port channel interface affects all physical interfaces that are assigned to that interface.

EtherChannel Operation

AutoNegotiation Protocols

EtherChannels can be formed through negotiation using one of two protocols, Port Aggregation Protocol (PAgP) or Link Aggregation Control Protocol (LACP). These protocols allow ports with similar characteristics to form a channel through dynamic negotiation with adjoining switches.

Note: It is also possible to configure a static or unconditional EtherChannel without PAgP or LACP.

EtherChannel Operation

PAgP Operation

PAgP (pronounced “Pag - P”) is a Cisco-proprietary protocol that aids in the automatic creation of EtherChannel links. When an EtherChannel link is configured using PAgP, PAgP packets are sent between EtherChannel-capable ports to negotiate the forming of a channel. When PAgP identifies matched Ethernet links, it groups the links into an EtherChannel. The EtherChannel is then added to the spanning tree as a single port.

When enabled, PAgP also manages the EtherChannel. PAgP packets are sent every 30 seconds. PAgP checks for configuration consistency and manages link additions and failures between two switches. It ensures that when an EtherChannel is created, all ports have the same type of configuration.

Note: In EtherChannel, it is mandatory that all ports have the same speed, duplex setting, and VLAN information. Any port modification after the creation of the channel also changes all other channel ports.

EtherChannel Operation

PAgP Operation (Cont.)

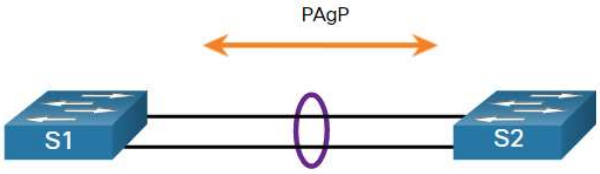
PAgP helps create the EtherChannel link by detecting the configuration of each side and ensuring that links are compatible so that the EtherChannel link can be enabled when needed. The modes for PAgP as follows:

- **On** - This mode forces the interface to channel without PAgP. Interfaces configured in the on mode do not exchange PAgP packets.
- **PAgP desirable** - This PAgP mode places an interface in an active negotiating state in which the interface initiates negotiations with other interfaces by sending PAgP packets.
- **PAgP auto** - This PAgP mode places an interface in a passive negotiating state in which the interface responds to the PAgP packets that it receives but does not initiate PAgP negotiation.

The modes must be compatible on each side. If one side is configured to be in auto mode, it is placed in a passive state, waiting for the other side to initiate the EtherChannel negotiation. If the other side is also set to auto, the negotiation never starts and the EtherChannel does not form. If all modes are disabled by using the **no** command, or if no mode is configured, then the EtherChannel is disabled. The on mode manually places the interface in an EtherChannel, without any negotiation. It works only if the other side is also set to on. If the other side is set to negotiate parameters through PAgP, no EtherChannel forms, because the side that is set to on mode does not negotiate. No negotiation between the two switches means there is no checking to make sure that all the links in the EtherChannel are terminating on the other side, or that there is PAgP compatibility on the other switch.

EtherChannel Operation

PAgP Mode Settings Example



The table shows the various combination of PAgP modes on S1 and S2 and the resulting channel establishment

S1	S2	Channel Establishment
On	On	Yes
On	Desirable/Auto	No
Desirable	Desirable	Yes
Desirable	Auto	Yes
Auto	Desirable	Yes
Auto	Auto	No

EtherChannel Operation

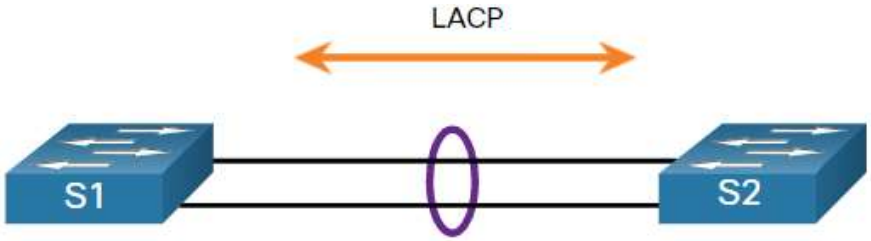
LACP Operation

LACP is part of an IEEE specification (802.3ad) that allows several physical ports to be bundled to form a single logical channel. LACP allows a switch to negotiate an automatic bundle by sending LACP packets to the other switch. It performs a function similar to PAgP with Cisco EtherChannel. Because LACP is an IEEE standard, it can be used to facilitate EtherChannels in multivendor environments. On Cisco devices, both protocols are supported.

LACP provides the same negotiation benefits as PAgP. LACP helps create the EtherChannel link by detecting the configuration of each side and making sure that they are compatible so that the EtherChannel link can be enabled when needed. The modes for LACP are as follows:

- **On** - This mode forces the interface to channel without LACP. Interfaces configured in the on mode do not exchange LACP packets.
- **LACP active** - This LACP mode places a port in an active negotiating state. In this state, the port initiates negotiations with other ports by sending LACP packets.
- **LACP passive** - This LACP mode places a port in a passive negotiating state. In this state, the port responds to the LACP packets that it receives but does not initiate LACP packet negotiation.

LACP Mode Settings Example



The table shows the various combination of LACP modes on S1 and S2 and the resulting channel establishment outcome.

S1	S2	Channel Establishment
On	On	Yes
On	Active/Passive	No
Active	Active	Yes
Active	Passive	Yes
Passive	Active	Yes
Passive	Passive	No

6.2 Configure EtherChannel

Configure EtherChannel

Configuration Guidelines

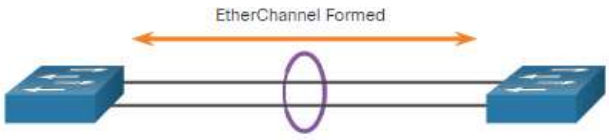
The following guidelines and restrictions are useful for configuring EtherChannel:

- **EtherChannel support** - All Ethernet interfaces must support EtherChannel with no requirement that interfaces be physically contiguous.
- **Speed and duplex** - Configure all interfaces in an EtherChannel to operate at the same speed and in the same duplex mode.
- **VLAN match** - All interfaces in the EtherChannel bundle must be assigned to the same VLAN or be configured as a trunk (shown in the figure).
- **Range of VLANs** - An EtherChannel supports the same allowed range of VLANs on all the interfaces in a trunking EtherChannel. If the allowed range of VLANs is not the same, the interfaces do not form an EtherChannel, even when they are set to **auto** or **desirable** mode.

Configure EtherChannel

Configuration Guidelines (Cont.)

- The figure shows a configuration that would allow an EtherChannel to form between S1 and S2.
- If these settings must be changed, configure them in port channel interface configuration mode. Any configuration that is applied to the port channel interface also affects individual interfaces. However, configurations that are applied to the individual interfaces do not affect the port channel interface. Therefore, making configuration changes to an interface that is part of an EtherChannel link may cause interface compatibility issues.
- The port channel can be configured in access mode, trunk mode (most common), or on a routed port.



S1 Port Configurations	
Speed	1 Gbps
Duplex	Full
VLAN	10

S2 Port Configurations	
Speed	1 Gbps
Duplex	Full
VLAN	10

Configure EtherChannel

LACP Configuration Example

Configuring EtherChannel with LACP requires the following three steps:

- **Step 1.** Specify the interfaces that compose the EtherChannel group using the **interface range** *interface* global configuration mode command. The **range** keyword allows you to select several interfaces and configure them all together.
- **Step 2.** Create the port channel interface with the **channel-group** *identifier* **mode active** command in interface range configuration mode. The identifier specifies a channel group number. The **mode active** keywords identify this as an LACP EtherChannel configuration.
- **Step3.** To change Layer 2 settings on the port channel interface, enter port channel interface configuration mode using the **interface port-channel** command, followed by the interface identifier. In the example, S1 is configured with an LACP EtherChannel. The port channel is configured as a trunk interface with the allowed VLANs specified.

```
S1(config)# interface range FastEthernet 0/1 - 2
S1(config-if-range)# channel-group 1 mode active
Creating a port-channel interface Port-channel 1
S1(config-if-range)# exit
S1(config-if)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 1,2,20
```


Configure EtherChannel

Packet Tracer – Configure EtherChannel

In this Packet Tracer, you will complete the following objectives:

- Configure Basic Switch Settings
- Configure an EtherChannel with Cisco PAgP
- Configure and 802.3ad EtherChannel
- Configure a Redundant EtherChannel Link

6.3 Verify and Troubleshoot EtherChannel

Verify and Troubleshoot EtherChannel

Verify EtherChannel

As always, when you configure devices in your network, you must verify your configuration. If there are problems, you will also need to be able to troubleshoot and fix them. There are a number of commands to verify an EtherChannel configuration:

- The **show interfaces port-channel** command displays the general status of the port channel interface.
- The **show etherchannel summary** command displays one line of information per port channel.
- The **show etherchannel port-channel** command displays information about a specific port channel interface.
- The **show interfaces etherchannel** command can provide information about the role of a physical member interface of the EtherChannel.

Verify and Troubleshoot EtherChannel

Common Issues with EtherChannel Configurations

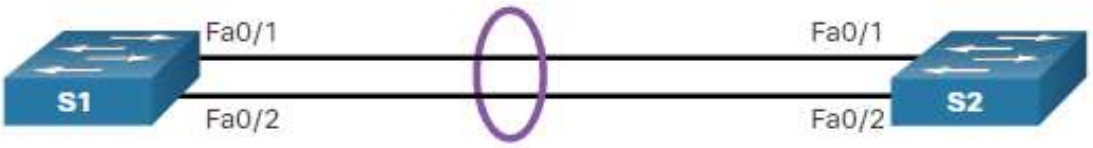
All interfaces within an EtherChannel must have the same configuration of speed and duplex mode, native and allowed VLANs on trunks, and access VLAN on access ports. Ensuring these configurations will significantly reduce network problems related to EtherChannel. Common EtherChannel issues include the following:

- Assigned ports in the EtherChannel are not part of the same VLAN, or not configured as trunks. Ports with different native VLANs cannot form an EtherChannel.
- Trunking was configured on some of the ports that make up the EtherChannel, but not all of them. It is not recommended that you configure trunking mode on individual ports that make up the EtherChannel. When configuring a trunk on an EtherChannel, verify the trunking mode on the EtherChannel.
- If the allowed range of VLANs is not the same, the ports do not form an EtherChannel even when PAgP is set to the **auto** or **desirable** mode.
- The dynamic negotiation options for PAgP and LACP are not compatibly configured on both ends of the EtherChannel.

Verify and Troubleshoot EtherChannel

Troubleshoot EtherChannel Example

In the figure, interfaces F0/1 and F0/2 on switches S1 and S2 are connected with an EtherChannel. However, the EtherChannel is not operational.



Verify and Troubleshoot EtherChannel

Troubleshoot EtherChannel Example (Cont.)

Step 1. View the EtherChannel Summary Information: The output of the **show etherchannel summary** command indicates that the EtherChannel is down.

```
S1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator
        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SD)         -      Fa0/1(D)    Fa0/2(D)
```


Verify and Troubleshoot EtherChannel

Troubleshoot EtherChannel Example (Cont.)

Step 2. View Port Channel Configuration: In the **show run | begin interface port-channel** output, more detailed output indicates that there are incompatible PAgP modes configured on S1 and S2.

```
S1# show run | begin interface port-channel
interface Port-channel1
 switchport trunk allowed vlan 1,2,20
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk allowed vlan 1,2,20
 switchport mode trunk
 channel-group 1 mode on
!
interface FastEthernet0/2
 switchport trunk allowed vlan 1,2,20
 switchport mode trunk
 channel-group 1 mode on
!==================================
S2# show run | begin interface port-channel
interface Port-channel1
 switchport trunk allowed vlan 1,2,20
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk allowed vlan 1,2,20
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/2
 switchport trunk allowed vlan 1,2,20
 switchport mode trunk
 channel-group 1 mode desirable
```

Troubleshoot EtherChannel Example (Cont.)

Step 3: Correct the Misconfiguration: To correct the issue, the PAgP mode on the EtherChannel is changed to desirable.

Note: EtherChannel and STP must interoperate. For this reason, the order in which EtherChannel-related commands are entered is important, which is why you see interface Port-Channel 1 removed and then re-added with the **channel-group** command, as opposed to directly changed. If one tries to change the configuration directly, STP errors cause the associated ports to go into blocking or errdisabled state.

```
S1(config)# no interface port-channel 1
S1(config)# interface range fa0/1 - 2
S1(config-if-range)# channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1
S1(config-if-range)# no shutdown
S1(config-if-range)# exit
S1(config)# interface range fa0/1 - 2
S1(config-if-range)# channel-group 1 mode desirable
S1(config-if-range)# no shutdown
S1(config-if-range)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```


Troubleshoot EtherChannel Example (Cont.)

Step 4. Verify EtherChannel is Operational: The EtherChannel is now active as verified by the output of the **show etherchannel summary** command.

```
S1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator
        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         PAgP      Fa0/1(P)    Fa0/2(P)
```

Verify and Troubleshoot EtherChannel

Packet Tracer – Troubleshoot EtherChannel

In this Packet Tracer, you will complete the following:

- Examine the Physical Layer and Correct Switch Port Mode Issues
- Identify and Correct Port Channel Assignment Issues
- Identify and Correct Port Channel Assignment Issues

Module 7: DHCPv4

Instructor Materials

Switching, Routing and Wireless Essentials v7.0 (SRWE)

Module Objectives

Module Title: DHCPv4

Module Objective: Implement DHCPv4 to operate across multiple LANs

Topic Title	Topic Objective
DHCP4 Concepts	Explain how DHCPv4 operates in a small- to medium-sized business network.
Configure a Cisco IOS DHCP4 Server	Configure a router as a DHCPv4 server.
Configure a DHCP4 Client	Configure a router as a DHCPv4 client.

7.1 DHCPv4 Concepts

DHCPv4 Concepts

DHCPv4 Server and Client

- Dynamic Host Configuration Protocol v4 (DHCPv4) assigns IPv4 addresses and other network configuration information dynamically. Because desktop clients typically make up the bulk of network nodes, DHCPv4 is an extremely useful and timesaving tool for network administrators.
- A dedicated DHCPv4 server is scalable and relatively easy to manage. However, in a small branch or SOHO location, a Cisco router can be configured to provide DHCPv4 services without the need for a dedicated server. Cisco IOS software supports an optional, full-featured DHCPv4 server.
- The DHCPv4 server dynamically assigns, or leases, an IPv4 address from a pool of addresses for a limited period of time chosen by the server, or until the client no longer needs the address.
- Clients lease the information from the server for an administratively defined period. Administrators configure DHCPv4 servers to set the leases to time out at different intervals. The lease is typically anywhere from 24 hours to a week or more. When the lease expires, the client must ask for another address, although the client is typically reassigned the same address.

DHCPv4 Concepts

DHCPv4 Operation

DHCPv4 works in a client/server mode. When a client communicates with a DHCPv4 server, the server assigns or leases an IPv4 address to that client.

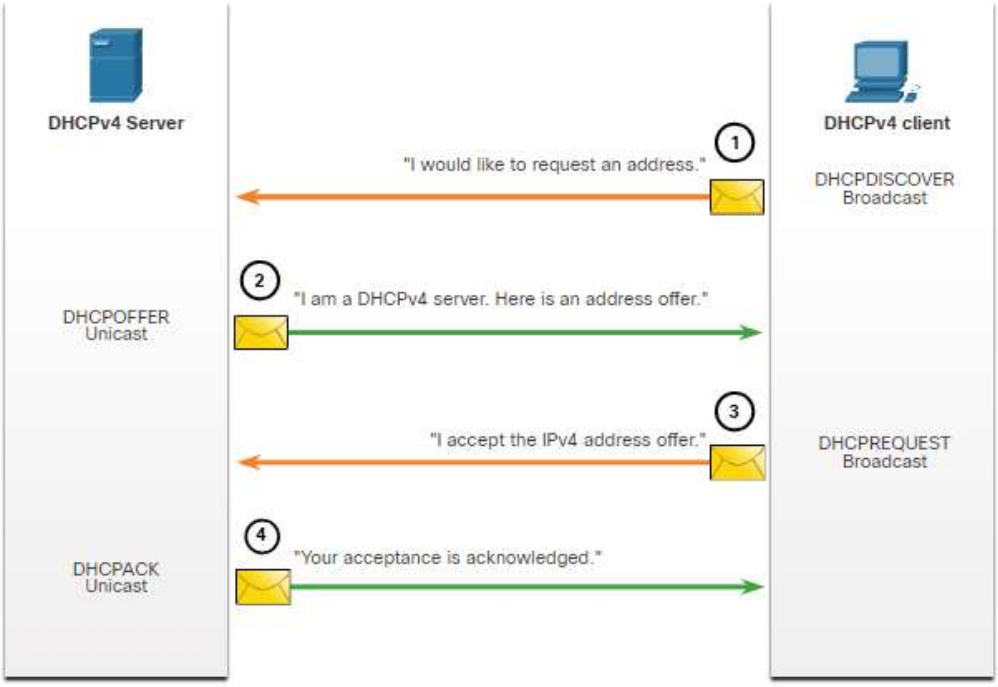
- The client connects to the network with that leased IPv4 address until the lease expires. The client must contact the DHCP server periodically to extend the lease.
- This lease mechanism ensures that clients that move or power off do not keep addresses that they no longer need.
- When a lease expires, the DHCP server returns the address to the pool where it can be reallocated as necessary.

DHCPv4 Concepts

Steps to Obtain a Lease

When the client boots (or otherwise wants to join a network), it begins a four-step process to obtain a lease:

1. DHCP Discover (DHCPDISCOVER)
2. DHCP Offer (DHCPOFFER)
3. DHCP Request (DHCPREQUEST)
4. DHCP Acknowledgment (DHCPACK)



DHCPv4 Concepts

Steps to Renew a Lease

Prior to lease expiration, the client begins a two-step process to renew the lease with the DHCPv4 server, as shown in the figure:

1. DHCP Request (DHCPREQUEST)
Before the lease expires, the client sends a DHCPREQUEST message directly to the DHCPv4 server that originally offered the IPv4 address. If a DHCPACK is not received within a specified amount of time, the client broadcasts another DHCPREQUEST so that one of the other DHCPv4 servers can extend the lease.

2. DHCP Acknowledgment (DHCPACK)
On receiving the DHCPREQUEST message, the server verifies the lease information by returning a DHCPACK.

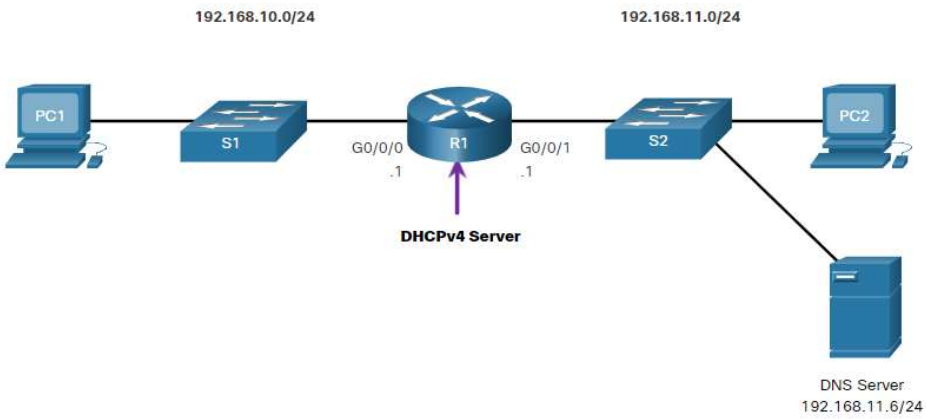
Note: These messages (primarily the DHCPOFFER and DHCPACK) can be sent as unicast or broadcast according to IETF RFC 2131.

7.2 Configure a Cisco IOS DHCPv4 Server

Configure a Cisco IOS DHCPv4 Server

Cisco IOS DHCPv4 Server

Now you have a basic understanding of how DHCPv4 works and how it can make your job a bit easier. A Cisco router running Cisco IOS software can be configured to act as a DHCPv4 server. The Cisco IOS DHCPv4 server assigns and manages IPv4 addresses from specified address pools within the router to DHCPv4 clients.



Configure a Cisco IOS DHCPv4 Server

Steps to Configure a Cisco IOS DHCPv4 Server

Use the following steps to configure a Cisco IOS DHCPv4 server:

- **Step 1**. Exclude IPv4 addresses. A single address or a range of addresses can be excluded by specifying the *low-address* and *high-address* of the range. Excluded addresses should be those addresses that are assigned to routers, servers, printers, and other devices that have been, or will be, manually configured. You can also enter the command multiple times. The command is **ip dhcp excluded-address *low-address [high-address]***
- **Step 2**. Define a DHCPv4 pool name. The **ip dhcp pool *pool-name*** command creates a pool with the specified name and puts the router in DHCPv4 configuration mode, which is identified by the prompt **Router(dhcp-config)#.**

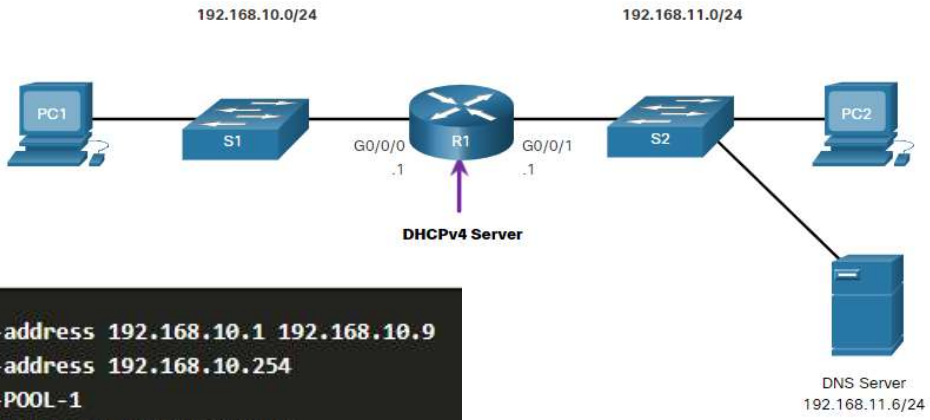
Configure a Cisco IOS DHCPv4 Server

Steps to Configure a Cisco IOS DHCPv4 Server (Cont.)

- **Step 3**. Configure the DHCPv4 pool. The address pool and default gateway router must be configured. Use the **network** statement to define the range of available addresses. Use the **default-router** command to define the default gateway router. These commands and other optional commands are shown in the table.

Task	IOS Command
Define the address pool.	**network** *network-number* [*mask* | / *prefix-length*]
Define the default router or gateway.	**default-router** address [*address2….address8*]
Define a DNS server.	**dns-server** *address* [*address2…address8*]
Define the domain name.	**domain-name** *domain*
Define the duration of the DHCP lease.	**lease** {*days* [*hours* [*minutes*]] | **infinite**}
Define the NetBIOS WINS server.	**netbios-name-server** *address* [*address2…address8*]

Configure a Cisco IOS DHCPv4 Server
Configuration Example




```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
R1#
```


Configure a Cisco IOS DHCPv4 Server
DHCPv4 Verification

Use the commands in the table to verify that the Cisco IOS DHCPv4 server is operational.

Command	Description
show running-config | section dhcp	Displays the DHCPv4 commands configured on the router.
show ip dhcp binding	Displays a list of all IPv4 address to MAC address bindings provided by the DHCPv4 service.
show ip dhcp server statistics	Displays count information regarding the number of DHCPv4 messages that have been sent and received

Configure a Cisco IOS DHCPv4 Server

Verify DHCPv4 is Operational

Verify the DHCPv4 Configuration: As shown in the example, the **show running-config | section dhcp** command output displays the DHCPv4 commands configured on R1. The **| section** parameter displays only the commands associated with DHCPv4 configuration.

```
R1# show running-config | section dhcp
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.254
ip dhcp pool LAN-POOL-1
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.168.11.5
 domain-name example.com
```


Configure a Cisco IOS DHCPv4 Server

Verify DHCPv4 is Operational (Cont.)

Verify DHCPv4 Bindings: As shown in the example, the operation of DHCPv4 can be verified using the **show ip dhcp binding** command. This command displays a list of all IPv4 address to MAC address bindings that have been provided by the DHCPv4 service.

```
R1# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/              Lease expiration        Type       State      Interface
                Hardware address/
                User name
192.168.10.10   0100.5056.b3ed.d8       Sep 15 2019 8:42 AM    Automatic  Active
GigabitEthernet0/0/0
```

Configure a Cisco IOS DHCPv4 Server

Verify DHCPv4 is Operational (Cont.)

Verify DHCPv4 Statistics: The output of the **show ip dhcp server statistics** is used to verify that messages are being received or sent by the router. This command displays count information regarding the number of DHCPv4 messages that have been sent and received.

```
R1# show ip dhcp server statistics
Memory usage         19465
Address pools        1
Database agents      0
Automatic bindings   2
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0
Renew messages       0
Workspace timeouts   0
Static routes        0
Relay bindings       0
Relay bindings active        0
Relay bindings terminated    0
Relay bindings selecting     0
Message              Received
BOOTREQUEST          0
DHCPDISCOVER         4
DHCPREQUEST          2
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0
```


Configure a Cisco IOS DHCPv4 Server

Verify DHCPv4 is Operational (Cont.)

Verify DHCPv4 Client Received IPv4 Addressing: The **ipconfig /all** command, when issued on PC1, displays the TCP/IP parameters, as shown in the example. Because PC1 was connected to the network segment 192.168.10.0/24, it automatically received a DNS suffix, IPv4 address, subnet mask, default gateway, and DNS server address from that pool. No DHCP-specific router interface configuration is required. If a PC is connected to a network segment that has a DHCPv4 pool available, the PC can obtain an IPv4 address from the appropriate pool automatically.

```
C:\Users\Student> ipconfig /all
Windows IP Configuration
   Host Name . . . . . . . . . . . . : ciscolab
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
Ethernet adapter Ethernet0:
   Connection-specific DNS Suffix  . : example.com
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : 00-05-9A-3C-7A-00
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained  . . . . . . . . . : Saturday, September 14, 2019 8:42:22AM
   Lease Expires   . . . . . . . . . : Sunday, September 15, 2019 8:42:22AM
   Default Gateway . . . . . . . . . : 192.168.10.1
   DHCP Server . . . . . . . . . . . : 192.168.10.1
   DNS Servers . . . . . . . . . . . : 192.168.11.5
```

Configure a Cisco IOS DHCPv4 Server

Disable the Cisco IOS DHCPv4 Server

The DHCPv4 service is enabled by default. To disable the service, use the **no service dhcp** global configuration mode command. Use the **service dhcp** global configuration mode command to re-enable the DHCPv4 server process, as shown in the example. Enabling the service has no effect if the parameters are not configured.

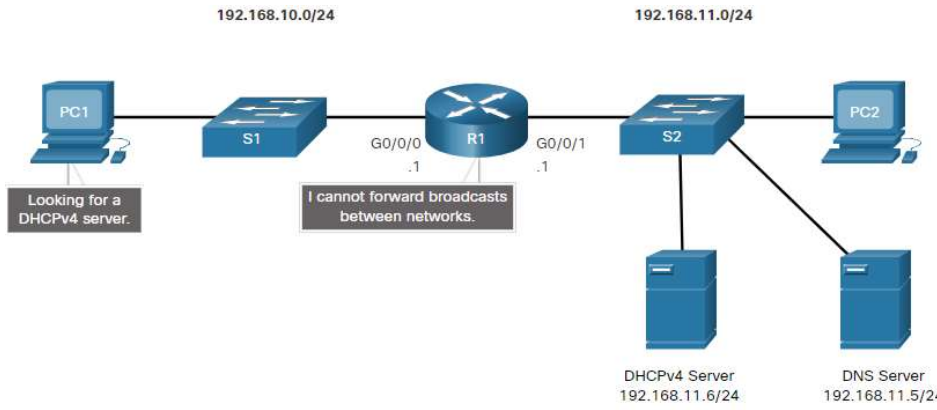
Note: Clearing the DHCP bindings or stopping and restarting the DHCP service may result in duplicate IP addresses being temporarily assigned on the network.

```
R1(config)# no service dhcp
R1(config)# service dhcp
R1(config)#
```


Configure a Cisco IOS DHCPv4 Server

DHCPv4 Relay

- In a complex hierarchical network, enterprise servers are usually located centrally. These servers may provide DHCP, DNS, TFTP, and FTP services for the network. Network clients are not typically on the same subnet as those servers. In order to locate the servers and receive services, clients often use broadcast messages.
- In the figure, PC1 is attempting to acquire an IPv4 address from a DHCPv4 server using a broadcast message. In this scenario, R1 is not configured as a DHCPv4 server and does not forward the broadcast. Because the DHCPv4 server is located on a different network, PC1 cannot receive an IP address using DHCP. R1 must be configured to relay DHCPv4 messages to the DHCPv4 server.



Configure a Cisco IOS DHCPv4 Server

DHCPv4 Relay (Cont.)

- Configure R1 with the **ip helper-address** *address* interface configuration command. This will cause R1 to relay DHCPv4 broadcasts to the DHCPv4 server. As shown in the example, the interface on R1 receiving the broadcast from PC1 is configured to relay DHCPv4 address to the DHCPv4 server at 192.168.11.6.
- When R1 has been configured as a DHCPv4 relay agent, it accepts broadcast requests for the DHCPv4 service and then forwards those requests as a unicast to the IPv4 address 192.168.11.6. The network administrator can use the **show ip interface** command to verify the configuration.

```
R1(config)# interface g0/0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1#
```

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.11.6
(output omitted)
```


Configure a Cisco IOS DHCPv4 Server

Other Service Broadcasts Relayed

DHCPv4 is not the only service that the router can be configured to relay. By default, the **ip helper-address** command forwards the following eight UDP services:

- Port 37: Time
- Port 49: TACACS
- Port 53: DNS
- Port 67: DHCP/BOOTP server
- Port 68: DHCP/BOOTP client
- Port 69: TFTP
- Port 137: NetBIOS name service
- Port 138: NetBIOS datagram service

Packet Tracer – Configure DHCPv4

In this Packet Tracer Activity, you will complete the following objectives:

- Part 1: Configure a Router as a DHCP Server
- Part 2: Configure DHCP Relay
- Part 3: Configure a Router as a DHCP Client
- Part 4: Verify DHCP and Connectivity

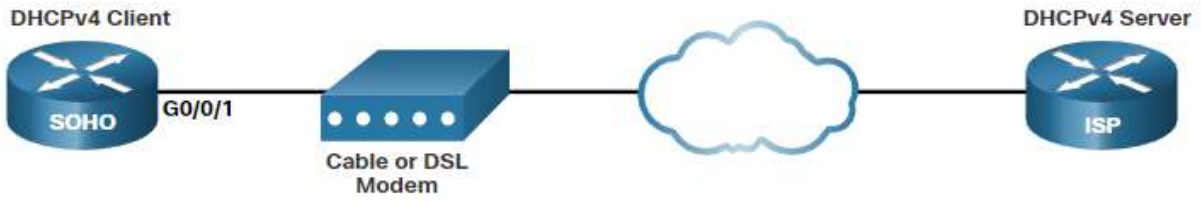
7.3 Configure a DHCPv4 Client

Configure a DHCPv4 Client

Cisco Router as a DHCPv4 Client

There are scenarios where you might have access to a DHCP server through your ISP. In these instances, you can configure a Cisco IOS router as a DHCPv4 client.

- Sometimes, Cisco routers in a small office or home office (SOHO) and branch sites have to be configured as DHCPv4 clients in a similar manner to client computers. The method used depends on the ISP. However, in its simplest configuration, the Ethernet interface is used to connect to a cable or DSL modem.
- To configure an Ethernet interface as a DHCP client, use the **ip address dhcp interface** configuration mode command.
- In the figure, assume that an ISP has been configured to provide select customers with IP addresses from the 209.165.201.0/27 network range after the G0/0/1 interface is configured with the **ip address dhcp** command.



Configure a DHCPv4 Client

Configuration Example

- To configure an Ethernet interface as a DHCP client, use the **ip address dhcp** interface configuration mode command, as shown in the example. This configuration assumes that the ISP has been configured to provide select customers with IPv4 addressing information.
- The **show ip interface g0/1** command confirms that the interface is up and that the address was allocated by a DHCPv4 server.

```
SOHO(config)# interface G0/0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
Sep 12 10:01:25.773: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0/0/1 assigned DHCP address
209.165.201.12, mask 255.255.255.224, hostname SOHO
```

```
SOHO# show ip interface g0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP
(output omitted)
```

Home Router as a DHCPv4 Client

Home routers are typically already set to receive IPv4 addressing information automatically from the ISP. This is so that customers can easily set up the router and connect to the internet.

- For example, the figure shows the default WAN setup page for a Packet Tracer wireless router. Notice that the internet connection type is set to **Automatic Configuration - DHCP**. This selection is used when the router is connected to a DSL or cable modem and acts as a DHCPv4 client, requesting an IPv4 address from the ISP.
- Various manufacturers of home routers will have a similar setup.

Module 8: SLAAC and DHCPv6

Instructor Materials

Switching, Routing and Wireless Essentials v7.0 (SRWE)

Module Objectives

Module Title: SLAAC and DHCPv6

Module Objective: Configure dynamic address allocation in IPv6 networks.

Topic Title	Topic Objective
IPv6 Global Unicast Address Assignment	Explain how an IPv6 host can acquire its IPv6 configuration.
SLAAC	Explain the operation of SLAAC.
DHCPv6	Explain the operation of DHCPv6
Configure DHCPv6 Server	Configure a stateful and stateless DHCPv6 server.

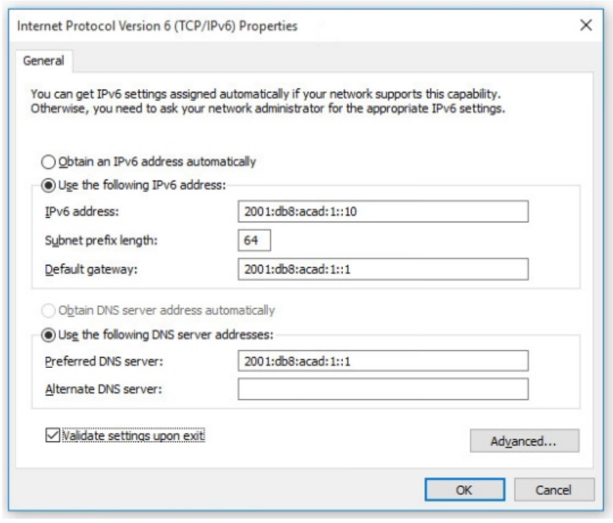
8.1 IPv6 GUA Assignment

IPv6 GUA Assignment

IPv6 Host Configuration

On a router, an IPv6 global unicast address (GUA) is manually configured using the **ipv6 address** *ipv6-address/prefix-length* interface configuration command.

- A Windows host can also be manually configured with an IPv6 GUA address configuration, as shown in the figure.
- However, manually entering an IPv6 GUA can be time consuming and somewhat error prone.
- Therefore, most Windows host are enabled to dynamically acquire an IPv6 GUA configuration.



IPv6 GUA Assignment

IPv6 Host Link-Local Address

If automatic IPv6 addressing is selected, the host will use an Internet Control Message Protocol version 6 (ICMPv6) Router Advertisement (RA) message to help it autoconfigure an IPv6 configuration.

- The IPv6 link-local address is automatically created by the host when it boots and the Ethernet interface is active.
- The interface did not create an IPv6 GUA in the output because the network segment did not have a router to provide network configuration instructions for the host.

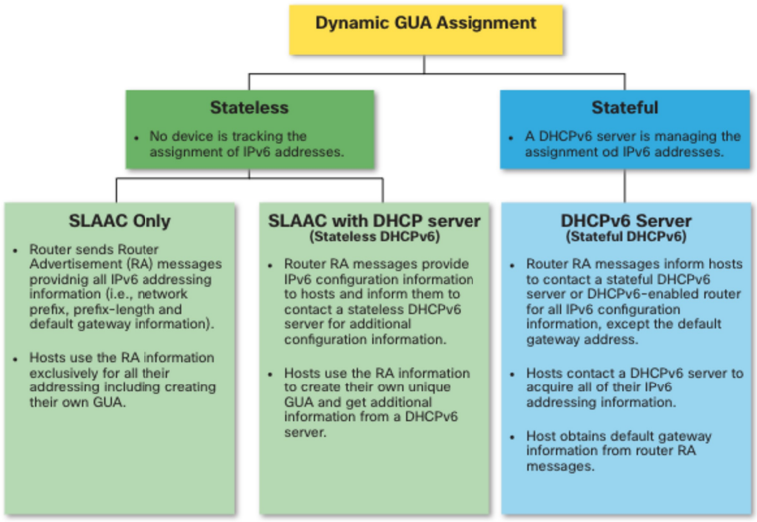
```
C:\PC1> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . :
   Link-local IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21
   IPv4 Address. . . . . . . . . . . : 169.254.202.140
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
C:\PC1>
```

- **Note:** The "%" and number at the end of the link-local address is known as a Zone ID or Scope ID and is used by the OS to associate the LLA with a specific interface.
- **Note**: DHCPv6 is defined in RFC 3315.

IPv6 GUA Assignment

By default, an IPv6-enabled router periodically send ICMPv6 RAs which simplifies how a host can dynamically create or acquire its IPv6 configuration.

- A host can dynamically be assigned a GUA using stateless and stateful services.
- All stateless and stateful methods in this module use ICMPv6 RA messages to suggest to the host how to create or acquire its IPv6 configuration.
- Although host operating systems follow the suggestion of the RA, the actual decision is ultimately up to the host

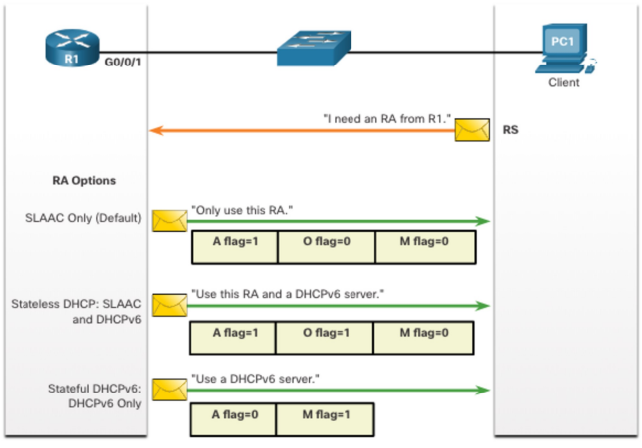


Three RA Message Flags

How a client obtains an IPv6 GUA depends on settings in the RA message.

An ICMPv6 RA message includes the following three flags:

- **A flag** - The Address Autoconfiguration flag signifies to use Stateless Address Autoconfiguration (SLAAC) to create an IPv6 GUA
- **O flag** - The Other Configuration flag signifies that additional information is available from a stateless DHCPv6 server.
- **M flag** - The Managed Address Configuration flag signifies to use a stateful DHCPv6 server to obtain an IPv6 GUA.



Using different combinations of the A, O and M flags, RA messages inform the host about the dynamic options available.

8.2 SLAAC

SLAAC
SLAAC Overview

Not every network has access to a DHCPv6 server but every device in an IPv6 network needs a GUA. The SLAAC method enables hosts to create their own unique IPv6 global unicast address without the services of a DHCPv6 server.

- SLAAC is a stateless service which means there is no server that maintains network address information to know which IPv6 addresses are being used and which ones are available.
- SLAAC sends periodic ICMPv6 RA messages (i.e., every 200 seconds) providing addressing and other configuration information for hosts to autoconfigure their IPv6 address based on the information in the RA.
- A host can also send a Router Solicitation (RS) message requesting an RA.
- SLAAC can be deployed as SLAAC only, or SLAAC with DHCPv6.

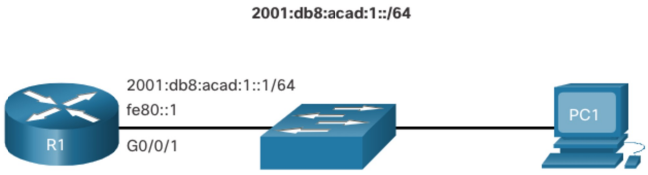
SLAAC

Enabling SLAAC

R1 G0/0/1 has been configured with the indicated IPv6 GUA and link-local addresses.

The R1 G0/0/01 IPv6 addresses include:

- **Link-local IPv6 address** - fe80::1
- **GUA / subnet** - 2001:db8:acad:1::1, 2001:db8:acad:1::/64
- **IPv6 all-nodes group** - ff02::1




```
R1# show ipv6 interface G0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Description: Link to LAN
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
(output omitted)
R1#
```

```
R1(config)# ipv6 unicast-routing
R1(config)# exit
R1#
```

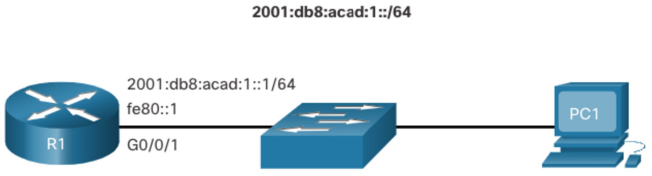
R1 is configured to join the all IPv6 multicast group and start sending RA messages containing address configuration information to hosts using SLAAC.

SLAAC

Enabling SLAAC (Cont.)

The IPv6 all-routers group responds to the IPv6 multicast address ff02::2.

- The **show ipv6 interface** command verifies that R1 has joined the IPv6 all-routers group (i.e., ff02::2).
- R1 will now begin to send RA messages every 200 seconds to the IPv6 all-nodes multicast address ff02::1.




```
R1# show ipv6 interface G0/0/1 | section Joined
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
R1#
```

SLAAC

SLAAC Only Method

RA messages from R1 have the following flags set:

- **A = 1** – Informs the client to use the IPv6 GUA prefix in the RA and dynamically create its own Interface ID.
- **O = 0** and **M = 0** – Informs the client to also use the additional information in the RA message (i.e., DNS server, MTU, and default gateway information).

- The **ipconfig** Windows command confirms that PC1 has generated an IPv6 GUS using the R1 RA.
- The default gateway address is LLA of the R1 G0/0/1 interface.

```
C:\PC1> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:1de9:c69:73ee:ca8c
   Link-local IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21
   IPv4 Address. . . . . . . . . . . : 169.254.202.140
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::1%6
C:\PC1>
```


SLAAC

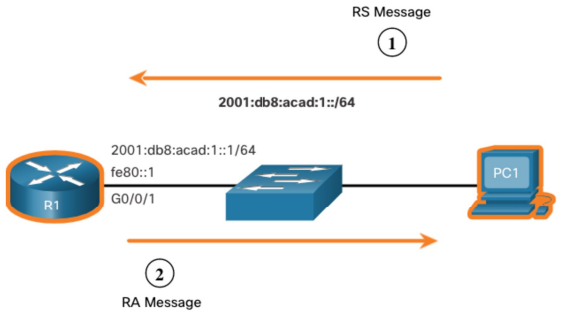
ICMPv6 RS Messages

A router sends RA messages every 200 seconds or when it receives an RS message from a host.

- IPv6 enabled hosts wishing to obtain IPv6 addressing information send an RS message to the IPv6 all-routers multicast address of ff02::2.

The figure illustrates how a host initiates the SLAAC method.

1. PC1 has just booted and sends an RS message to the IPv6 all-routers multicast address of ff02::2 requesting an RA.
2. R1 generates an RA and then sends the RA message to the IPv6 all-nodes multicast address of ff02::1. PC1 uses this information to create a unique IPv6 GUA.



SLAAC
Host Process to Generate Interface ID

Using SLAAC, a host acquires its 64-bit IPv6 subnet information from the router RA and must generate the remainder 64-bit interface identifier (ID) using either:

- **Randomly generated** - The 64-bit interface ID is randomly generated by the client operating system. This is the method now used by Windows 10 hosts.
- **EUI-64** - The host creates an interface ID using its 48-bit MAC address and inserts the hex value of fffe in the middle of the address. Some operating systems default to the randomly generated interface ID instead of the EUI-64 method, due to privacy concerns. This is because the Ethernet MAC address of the host is used by EUI-64 to create the interface ID.

Note: Windows, Linux, and Mac OS allow for the user to modify the generation of the interface ID to be either randomly generated or to use EUI-64.

SLAAC
Duplicate Address Detection

A SLAAC host may use the following Duplicate Address Detection (DAD) process to ensure that the IPv6 GUA is unique.

- The host sends an ICMPv6 Neighbor Solicitation (NS) message with a specially constructed solicited-node multicast address containing the last 24 bits of IPv6 address of the host.
- If no other devices respond with a Neighbor Advertisement (NA) message, then the address is virtually guaranteed to be unique and can be used by the host.
- If an NA is received by the host, then the address is not unique, and the host must generate a new interface ID to use.

Note: DAD is really not required because a 64-bit interface ID provides 18 quintillion possibilities. Therefore, the chance of a duplicate address is remote. However, the Internet Engineering Task Force (IETF) recommends that DAD is used. Therefore, most operating systems perform DAD on all IPv6 unicast addresses, regardless of how the address is configured.

8.3 DHCPv6

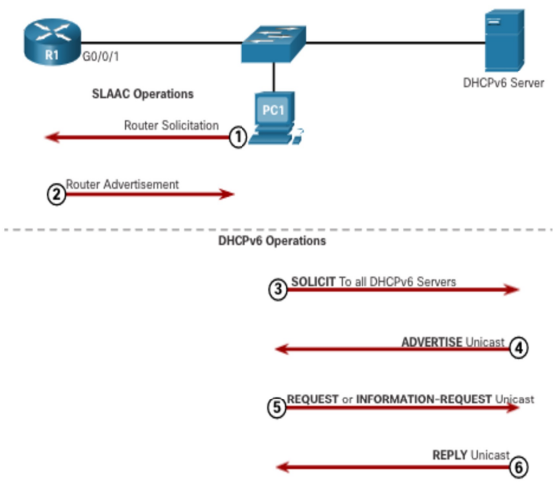
DHCPv6

DHCPv6 Operation Steps

Stateful DHCPv6 does not require SLAAC while stateless DHCPv6 does.

Regardless, when an RA indicates to use DHCPv6 or stateful DHCPv6:

1. The host sends an RS message.
2. The router responds with an RA message.
3. The host sends a DHCPv6 SOLICIT message.
4. The DHCPv6 server responds with an ADVERTISE message.
5. The host responds to the DHCPv6 server.
6. The DHCPv6 server sends a REPLY message.



Note: Server to client DHCPv6 messages use UDP destination port 546 while client to server DHCPv6 messages use UDP destination port 547.

DHCPv6

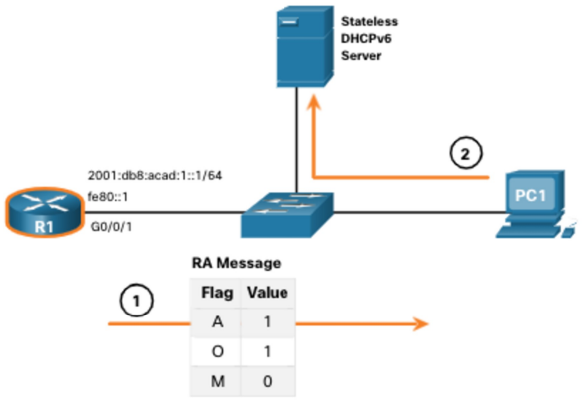
Stateless DHCPv6 Operation

If an RA indicates the stateless DHCPv6 method, the host uses the information in the RA message for addressing and contacts a DHCPv6 server for additional information.

Note: The DHCPv6 server only provides configuration parameters for clients and does not maintain a list of IPv6 address bindings (i.e. stateless).

For example, PC1 receives a stateless RA message containing:

- The IPv6 GUA network prefix and prefix length.
- A flag set to 1 informing the host to use SLAAC.
- O flag set to 1 informing the host to seek that additional configuration information from a DHCPv6 server.
- M flag set to the default value 0.



- PC1 sends a DHCPv6 SOLICIT message seeking additional information from a stateless DHCPv6 server.

DHCPv6

Enable Stateless DHCPv6 on an Interface

Stateless DHCPv6 is enabled using the **ipv6 nd other-config-flag** interface configuration command setting the O flag to 1.

The highlighted output confirms the RA will tell receiving hosts to use stateless autoconfigure (A flag = 1) and contact a DHCPv6 server to obtain another configuration information (O flag = 1).

Note: You can use the **no ipv6 nd other-config-flag** to reset the interface to the default SLAAC only option (O flag = 0).

```
R1(config-if)# ipv6 nd other-config-flag
R1(config-if)# end
R1#
R1# show ipv6 interface g0/0/1 | begin ND
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
  Hosts use DHCP to obtain other configuration.
R1#
```


DHCPv6

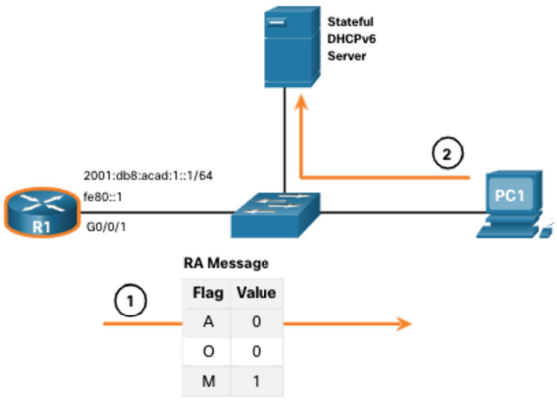
Stateful DHCPv6 Operation

If an RA indicates the stateful DHCPv6 method, the host contacts a DHCPv6 server for all configuration information.

- **Note**: The DHCPv6 server is stateful and maintains a list of IPv6 address bindings.

For example, PC1 receives a stateful RA message containing:

- The IPv6 GUA network prefix and prefix length.
- A flag set to 0 informing the host to contact a DHCPv6 server.
- O flag set to 0 informing the host to contact a DHCPv6 server.
- M flag set to the value 1.



- PC1 sends a DHCPv6 SOLICIT message seeking additional information from a stateful DHCPv6 server.

DHCPv6

Enable Stateful DHCPv6 on an Interface

Stateful DHCPv6 is enabled using the **ipv6 nd managed-config-flag** interface configuration command setting the M flag to 1.

The highlighted output in the example confirms that the RA will tell the host to obtain all IPv6 configuration information from a DHCPv6 server (M flag = 1).

```
R1(config)# int g0/0/1
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# end
R1#
R1# show ipv6 interface g0/0/1 | begin ND
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use DHCP to obtain routable addresses.
R1#
```

8.4 Configure DHCPv6 Server

Configure DHCPv6 Server

DHCPv6 Router Roles

Cisco IOS routers are powerful devices. In smaller networks, you do not have to have separate devices to have a DHCPv6 server, client, or relay agent. A Cisco IOS router can be configured to provide DHCPv6 server services.

Specifically, it can be configured to be one of the following:

- **DHCPv6 Server** - Router provides stateless or stateful DHCPv6 services.
- **DHCPv6 Client** - Router interface acquires an IPv6 IP configuration from a DHCPv6 server.
- **DHCPv6 Relay Agent** - Router provides DHCPv6 forwarding services when the client and the server are located on different networks.

Configure DHCPv6 Server

Configure a Stateless DHCPv6 Server

The stateless DHCPv6 server option requires that the router advertise the IPv6 network addressing information in RA messages.

There are five steps to configure and verify a router as a stateless DHCPv6 server:

1. Enable IPv6 routing using the **ipv6 unicast-routing** command.
2. Define a DHCPv6 pool name using the **ipv6 dhcp pool** *POOL-NAME* global config command.
3. Configure the DHCPv6 pool with options. Common options include **dns-server X:X:X:X:X:X:X:X** and **domain-name *name***.
4. Bind the interface to the pool using the **ipv6 dhcp server** *POOL-NAME* interface config command.
   - Manually change the O flag from 0 to 1 using the ipv6 nd other-config-flag interface command. RA messages sent on this interface indicate that additional information is available from a stateless DHCPv6 server. The A flag is 1 by default, telling clients to use SLAAC to create their own GUA.
5. Verify that the hosts have received IPv6 addressing information using the **ipconfig /all** command.

Configure DHCPv6 Server

Configure a Stateless DHCPv6 Client

A router can also be a DHCPv6 client and get an IPv6 configuration from a DHCPv6 server, such as a router functioning as a DHCPv6 server.

1. Enable IPv6 routing using the **ipv6 unicast-routing** command.
2. Configure the client router to create an LLA. An IPv6 link-local address is created on a router interface when a global unicast address is configured, or without a GUA using the **ipv6 enable** interface configuration command. Cisco IOS uses EUI-64 to create the Interface ID.
3. Configure the client router to use SLAAC using the **ipv6 address autoconfig** command.
4. Verify that the client router is assigned a GUA using the **show ipv6 interface brief** command.
5. Verify that the client router received other necessary DHCPv6 information. The **show ipv6 dhcp interface g0/0/1** command confirms DHCP option information, such as DNS server and domain name, have been received by the client.

Configure DHCPv6 Server

Configure a Stateful DHCPv6 Server

The stateful DHCP server option requires that the IPv6 enabled router tells the host to contact a DHCPv6 server to obtain all necessary IPv6 network addressing information.

There are five steps to configure and verify a router as a stateful DHCPv6 server:

1. Enable IPv6 routing using the **ipv6 unicast-routing** command.
2. Define a DHCPv6 pool name using the **ipv6 dhcp pool** *POOL-NAME* global config command.
3. Configure the DHCPv6 pool with options. Common options include the **address prefix** command, domain name, DHS server IP address, and more.
4. Bind the interface to the pool using the **ipv6 dhcp server** *POOL-NAME* interface config command.
   - Manually change the M flag from 0 to 1 using the interface command **ipv6 nd managed-config-flag**.
   - Manually change the A flag from 1 to 0 using the **ipv6 nd prefix default no-autoconfig** interface command to inform the client to not to use SLAAC to create a GUA. The router will now respond to stateful DHCPv6 requests with the information contained in the pool.
5. Verify that the hosts have received IPv6 addressing information using the **ipconfig /all** command.

Configure DHCPv6 Server

Configure a Stateful DHCPv6 Client

A router can also be a DHCPv6 client. The client router needs to have **ipv6 unicast-routing** enabled and an IPv6 link-local address to send and receive IPv6 messages.

There are five steps to configure and verify a router as a stateless DHCPv6 client.

1. Enable IPv6 routing using the **ipv6 unicast-routing** command.
2. Configure the client router to create an LLA. An IPv6 link-local address is created on a router interface when a global unicast address is configured, or without a GUA using the **ipv6 enable** interface configuration command. Cisco IOS uses EUI-64 to create an Interface ID.
3. Configure the client router to use DHCPv6 using the **ipv6 address dhcp** interface config command.
4. Verify that the client router is assigned a GUA using the **show ipv6 interface brief** command.
5. Verify that the client router received other necessary DHCPv6 information using the **show ipv6 dhcp interface g0/0/1** command.

Configure DHCPv6 Server

DHCPv6 Server Verification Commands

The **show ipv6 dhcp pool** command verifies the name of the DHCPv6 pool and its parameters. The command also identifies the number of active clients.

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6-STATEFUL
  Address allocation prefix: 2001:DB8:ACAD:1::/64 valid 172800 preferred 86400 (2 in use,  0
conflicts)
  DNS server: 2001:4860:4860::8888
  Domain name: example.com
  Active clients: 2
R1#
```


Configure DHCPv6 Server

DHCPv6 Server Verification Commands (Cont.)

Use the **show ipv6 dhcp binding** command output to display the IPv6 link-local address of the client and the global unicast address assigned by the server.

- This information is maintained by a stateful DHCPv6 server.
- A stateless DHCPv6 server would not maintain this information.

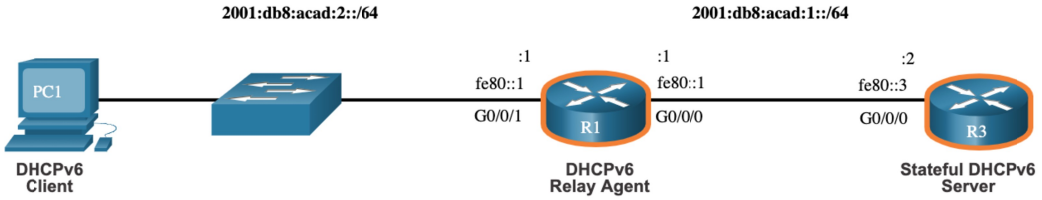
```
R1# show ipv6 dhcp binding
Client: FE80::192F:6FBC:9DB:B749
  DUID: 0001000125148183005056B327D6
  Username : unassigned
  VRF : default
  IA NA: IA ID 0x03000C29, T1 43200, T2 69120
    Address: 2001:DB8:ACAD:1:A43C:FD28:9D79:9E42
             preferred lifetime 86400, valid lifetime 172800
             expires at Sep 27 2019 09:10 AM (171192 seconds)
Client: FE80::2FC:BAFF:FE94:29B1
  DUID: 0003000100FCBA9429B0
  Username : unassigned
  VRF : default
  IA NA: IA ID 0x00060001, T1 43200, T2 69120
    Address: 2001:DB8:ACAD:1:B4CB:25FA:3C9:747C
             preferred lifetime 86400, valid lifetime 172800
             expires at Sep 27 2019 09:29 AM (172339 seconds)
R1#
```

Configure DHCPv6 Server

Configure a DHCPv6 Relay Agent

If the DHCPv6 server is located on a different network than the client, then the IPv6 router can be configured as a DHCPv6 relay agent.

- The configuration of a DHCPv6 relay agent is similar to the configuration of an IPv4 router as a DHCPv4 relay.
- This command is configured on the interface facing the DHCPv6 clients and specifies the DHCPv6 server address and egress interface to reach the server, as shown in the output. The egress interface is only required when the next-hop address is an LLA.




```
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ipv6 dhcp relay destination 2001:db8:acad:1::2 G0/0/0
R1(config-if)# exit
R1(config)#
```


Configure DHCPv6 Server

Verify the DHCPv6 Relay Agent

Verify that the DHCPv6 relay agent is operational with the **show ipv6 dhcp interface** and **show ipv6 dhcp binding** commands.

```
R1# show ipv6 dhcp interface
GigabitEthernet0/0/1 is in relay mode
  Relay destinations:
    2001:DB8:ACAD:1::2
    2001:DB8:ACAD:1::2 via GigabitEthernet0/0/0
R1#
```

```
R3# show ipv6 dhcp binding
Client: FE80::5C43:EE7C:2959:DA68
  DUID: 0001000124F5CEA2005056B3636D
  Username : unassigned
  VRF : default
  IA NA: IA ID 0x03000C29, T1 43200, T2 69120
    Address: 2001:DB8:ACAD:2:9C3C:64DE:AADA:7857
             preferred lifetime 86400, valid lifetime 172800
             expires at Sep 29 2019 08:26 PM (172710 seconds)
R3#
```

Verify Windows hosts received IPv6 addressing information with the **ipconfig /all** command.

Module 9: FHRP Concepts

Instructor Materials

Switching, Routing and Wireless Essentials v7.0 (SRWE)

Module Objectives

Module Title: FHRP Concepts

Module Objective: Explain how FHRPs provide default gateway services in a redundant network.

Topic Title	Topic Objective
First Hop Redundancy Protocols	Explain the purpose and operation of first hop redundancy protocols.
HSRP	Explain how HSRP operates.

9.1 First Hop Redundancy Protocols

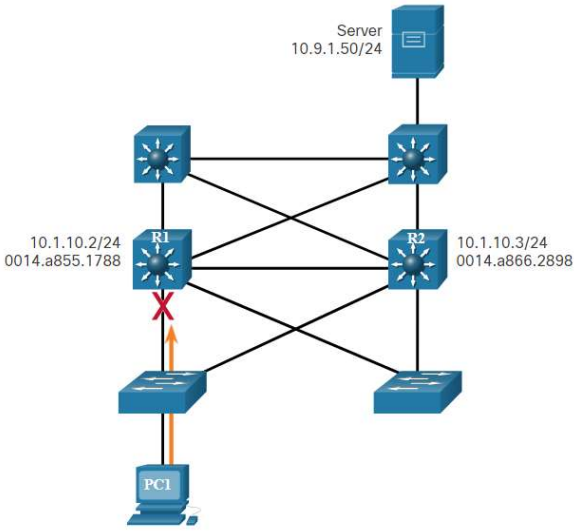
First Hop Redundancy Protocols

Default Gateway Limitations

End devices are typically configured with a single default gateway IPv4 address.

- If the default gateway router interface fails, LAN hosts lose outside LAN connectivity.
- This occurs even if a redundant router or Layer 3 switch that could serve as a default gateway exists.

First hop redundancy protocols (FHRPs) are mechanisms that provide alternate default gateways in switched networks where two or more routers are connected to the same VLANs.



First Hop Redundancy Protocols

Router Redundancy

One way to prevent a single point of failure at the default gateway is to implement a virtual router. To implement this type of router redundancy, multiple routers are configured to work together to present the illusion of a single router to the hosts on the LAN. By sharing an IP address and a MAC address, two or more routers can act as a single virtual router.

- The IPv4 address of the virtual router is configured as the default gateway for the workstations on a specific IPv4 segment.
- When frames are sent from host devices to the default gateway, the hosts use ARP to resolve the MAC address that is associated with the IPv4 address of the default gateway. The ARP resolution returns the MAC address of the virtual router. Frames that are sent to the MAC address of the virtual router can then be physically processed by the currently active router within the virtual router group.
- A protocol is used to identify two or more routers as the devices that are responsible for processing frames that are sent to the MAC or IP address of a single virtual router. Host devices send traffic to the address of the virtual router. The physical router that forwards this traffic is transparent to the host devices.

First Hop Redundancy Protocols

Router Redundancy (Cont.)

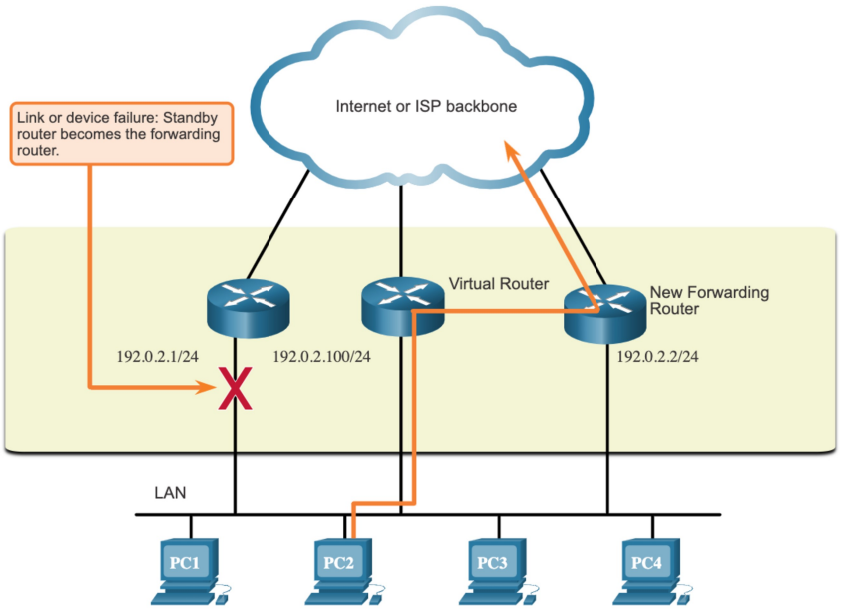
- A redundancy protocol provides the mechanism for determining which router should take the active role in forwarding traffic. It also determines when the forwarding role must be taken over by a standby router. The transition from one forwarding router to another is transparent to the end devices.
- The ability of a network to dynamically recover from the failure of a device acting as a default gateway is known as first-hop redundancy.

First Hop Redundancy Protocols

Steps for Router Failover

When the active router fails, the redundancy protocol transitions the standby router to the new active router role, as shown in the figure. These are the steps that take place when the active router fails:

1. The standby router stops seeing Hello messages from the forwarding router.
2. The standby router assumes the role of the forwarding router.
3. Because the new forwarding router assumes both the IPv4 and MAC addresses of the virtual router, the host devices see no disruption in service.



First Hop Redundancy Protocols

FHRP Options

FHRP Options	Description
Hot Standby Router Protocol (HSRP)	HRSP is a Cisco-proprietary FHRP that is designed to allow for transparent failover of a first-hop IPv4 device. HSRP is used in a group of routers for selecting an active device and a standby device. The active device is the device that is used for routing packets; the standby device is the device that takes over when the active device fails, or when pre-set conditions are met.
HSRP for IPv6	This is a Cisco-proprietary FHRP that provides the same functionality of HSRP, but in an IPv6 environment. An HSRP IPv6 group has a virtual MAC address derived from the HSRP group number and a virtual IPv6 link-local address derived from the HSRP virtual MAC address. Periodic router advertisements (RAs) are sent for the HSRP virtual IPv6 link-local address when the HSRP group is active. When the group becomes inactive, these RAs stop after a final RA is sent.
Virtual Router Redundancy Protocol version 2 (VRRPv2)	This is a non-proprietary election protocol that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on an IPv4 LAN. This allows several routers on a multiaccess link to use the same virtual IPv4 address. In a VRRP configuration, one router is elected as the virtual router master, with the other routers acting as backups, in case the virtual router master fails.
VRRPv3	This provides the capability to support IPv4 and IPv6 addresses. VRRPv3 works in multi-vendor environments and is more scalable than VRRPv2.
Gateway Load Balancing Protocol (GLBP)	This is a Cisco-proprietary FHRP that protects data traffic from a failed router or circuit, like HSRP and VRRP, while also allowing load balancing (also called load sharing) between a group of redundant routers.
GLBP for IPv6	This is a Cisco-proprietary FHRP that provides the same functionality of GLBP, but in an IPv6 environment. GLBP for IPv6 provides automatic router backup for IPv6 hosts configured with a single default gateway on a LAN. Multiple first-hop routers on the LAN combine to offer a single virtual first-hop IPv6 router while sharing the IPv6 packet forwarding load.
ICMP Router Discovery Protocol (IRDP)	Specified in RFC 1256, IRDP is a legacy FHRP solution. IRDP allows IPv4 hosts to locate routers that provide IPv4 connectivity to other (nonlocal) IP networks.

9.2 HSRP

HSRP
HSRP Overview

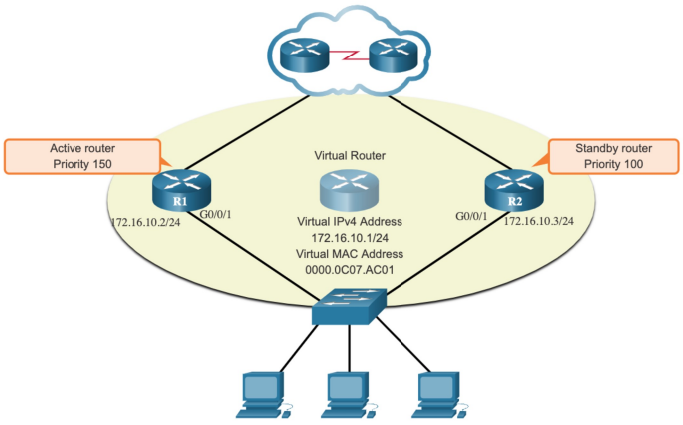
Cisco provides HSRP and HSRP for IPv6 as a way to avoid losing outside network access if your default router fails. HSRP is a Cisco-proprietary FHRP that is designed to allow for transparent failover of a first-hop IP device.

HSRP ensures high network availability by providing first-hop routing redundancy for IP hosts on networks configured with an IP default gateway address. HSRP is used in a group of routers for selecting an active device and a standby device. In a group of device interfaces, the active device is the device that is used for routing packets; the standby device is the device that takes over when the active device fails, or when pre-set conditions are met. The function of the HSRP standby router is to monitor the operational status of the HSRP group and to quickly assume packet-forwarding responsibility if the active router fails.

HSRP
HSRP Priority and Preemption

The role of the active and standby routers is determined during the HSRP election process. By default, the router with the numerically highest IPv4 address is elected as the active router. However, it is always better to control how your network will operate under normal conditions rather than leaving it to chance.

- HSRP priority can be used to determine the active router.
- The router with the highest HSRP priority will become the active router.
- By default, the HSRP priority is 100.
- If the priorities are equal, the router with the numerically highest IPv4 address is elected as the active router.
- To configure a router to be the active router, use the **standby priority** interface command. The range of the HSRP priority is 0 to 255.

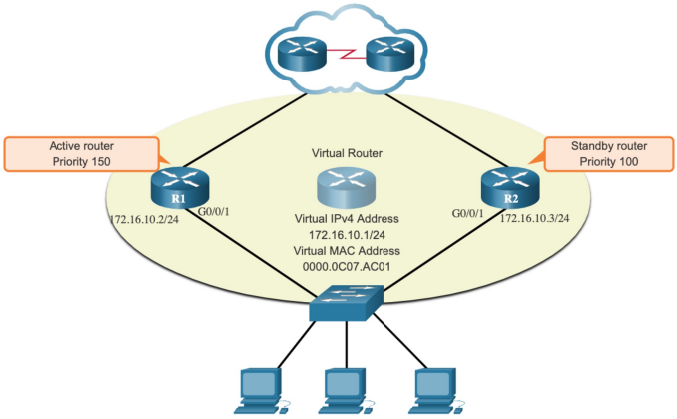


HSRP
HSRP Priority and Preemption (Cont.)

By default, after a router becomes the active router, it will remain the active router even if another router comes online with a higher HSRP priority.

- To force a new HSRP election process to take place when a higher priority router comes online, preemption must be enabled using the **standby preempt** interface command. Preemption is the ability of an HSRP router to trigger the re-election process. With preemption enabled, a router that comes online with a higher HSRP priority will assume the role of the active router.
- Preemption only allows a router to become the active router if it has a higher priority. A router enabled for preemption, with equal priority but a higher IPv4 address will not preempt an active router. Refer to the topology in the figure.

Note: With preemption disabled, the router that boots up first will become the active router if there are no other routers online during the election process.



HSRP States and Times

HSRP State	Description
Initial	This state is entered through a configuration change or when an interface first becomes available.
Learn	The router has not determined the virtual IP address and has not yet seen a hello message from the active router. In this state, the router waits to hear from the active router.
Listen	The router knows the virtual IP address, but the router is neither the active router nor the standby router. It listens for hello messages from those routers.
Speak	The router sends periodic hello messages and actively participates in the election of the active and/or standby router.
Standby	The router is a candidate to become the next active router and sends periodic hello messages.

The active and standby HSRP routers send hello packets to the HSRP group multicast address every 3 seconds by default. The standby router will become active if it does not receive a hello message from the active router after 10 seconds. You can lower these timer settings to speed up the failover or preemption. However, to avoid increased CPU usage and unnecessary standby state changes, do not set the hello timer below 1 second or the hold timer below 4 seconds.