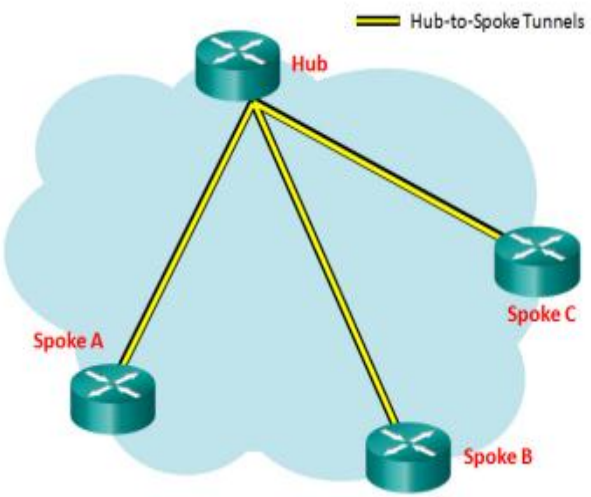
Parametros de calidad de servicio QoS, E-BGP y otros.

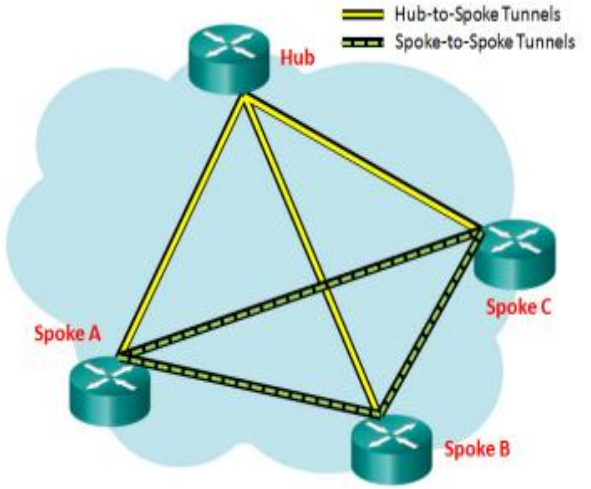
RAUL BAREÑO GUTIERREZ

Cisco | Networking Academy®
Mind Wide Open™

Tipos de VPN DMVPN

- Dynamic Multipoint VPN (DMVPN): solución de software de Cisco para la construcción de múltiples VPN de una manera fácil, dinámica y escalable.
- Simplifica la configuración y proporciona flexibilidad.
- topologías DMVPN que se pueden utilizar:
- Túneles hub a nodo
- túneles Hub-a-nodo y nodo a nodo
- DMVPN se construye a partir de las siguientes tecnologías:
- Protocolo de resolución del siguiente salto (NHRP)
- Multipunto encapsulación de enrutamiento genérico (mGRE) túneles
- Seguridad IP cifrado (IPsec)





eBGP

Cisco | Networking Academy®
Mind Wide Open™

Protocolos de Enrutamiento IGP and EGP

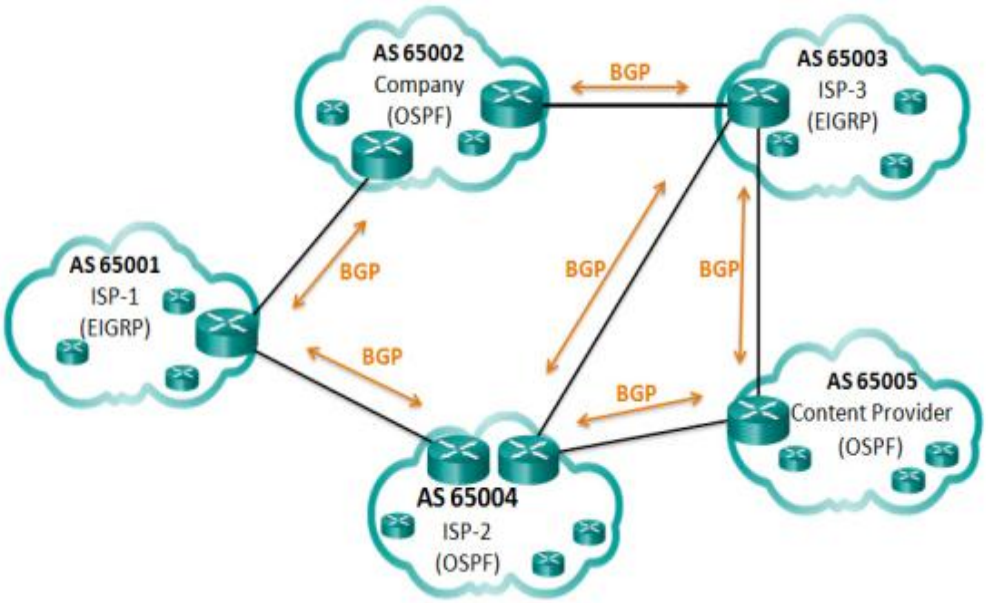
IGP se utilizan para intercambiar información de enrutamiento dentro de una red de la empresa o de un sistema autónomo (AS). RIP, EIGRP and OSPF.

Border Gateway Protocol (BGP) es un Exterior Gateway Protocol (EGP)

Se utiliza para enrutar entre las redes administradas por dos ISP diferentes.

En BGP, cada AS se le asigna un único número de 16 bits o de 32 bits que identifica de manera única en Internet.

Las Actualizaciones BGP se encapsulan a través de TCP en el puerto 179.



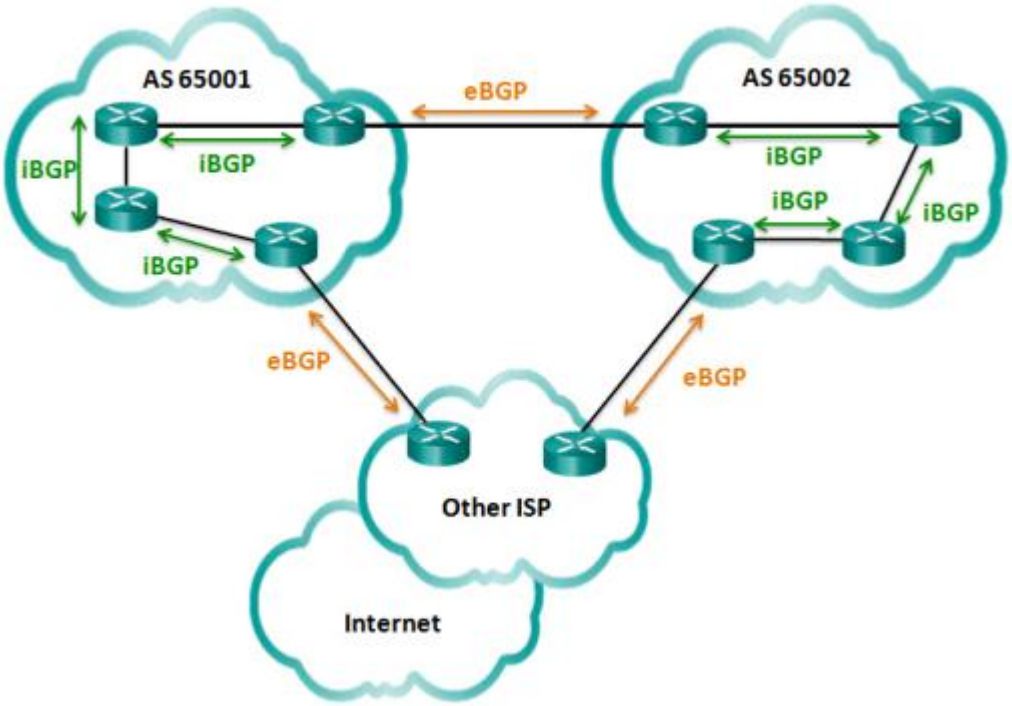
eBGP y iBGP

- Hay dos tipos de BGP:

- BGP externo (eBGP) - BGP externo es el protocolo de enrutamiento entre los routers utilizados en diferentes sistemas autónomos.

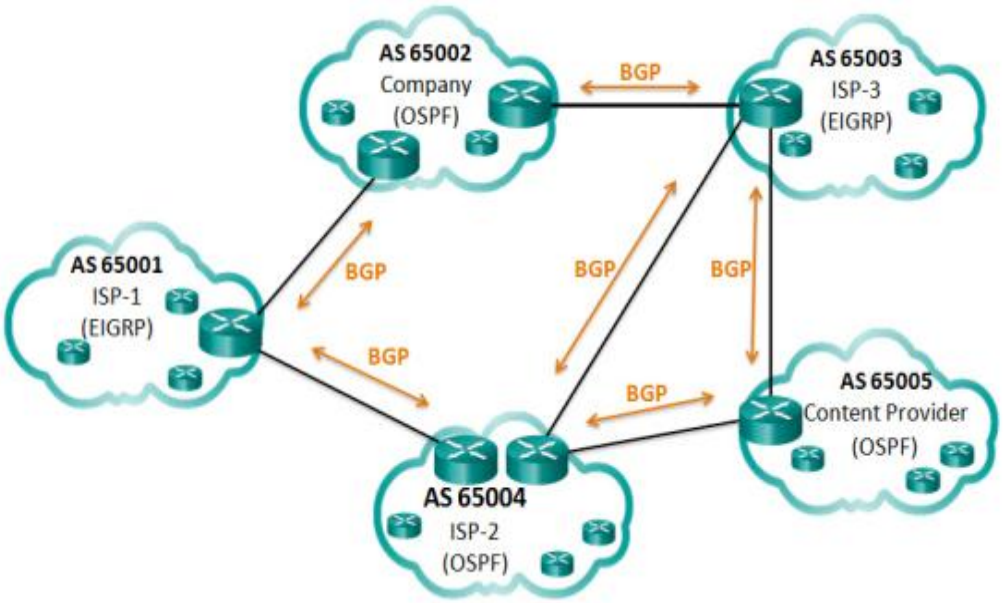
- BGP interno (iBGP) - BGP interno es el protocolo de enrutamiento utilizado entre routers en el mismo AS.

- Este curso se centra en eBGP.



Cuando usar BGP

- El uso de BGP es más apropiado cuando un AS tiene conexiones a múltiples sistemas autónomos.
- Esto se conoce como multi-homed.
- Antes de ejecutar BGP es importante también tener una buena comprensión de BGP.



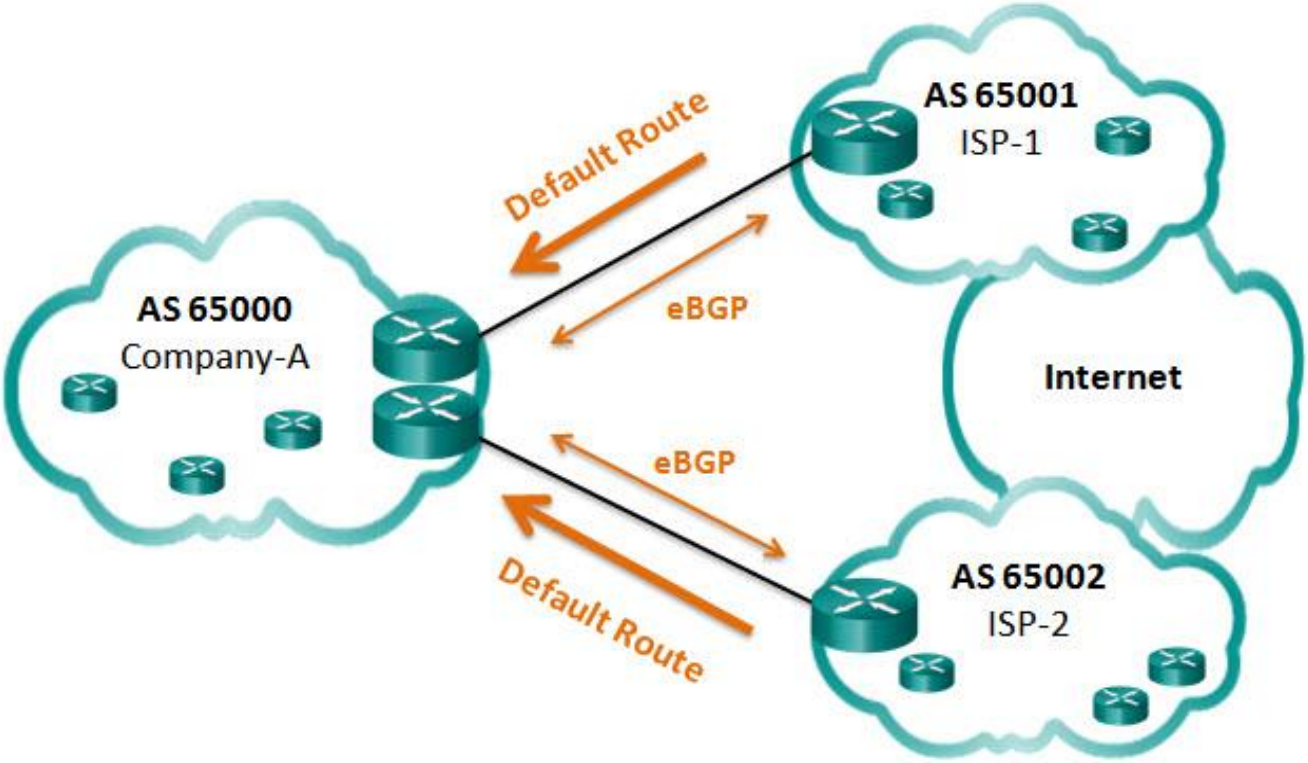
Opciones de BGP

- **única ruta por defecto**

  ISP anuncian una ruta predeterminada a la Compañía-A.

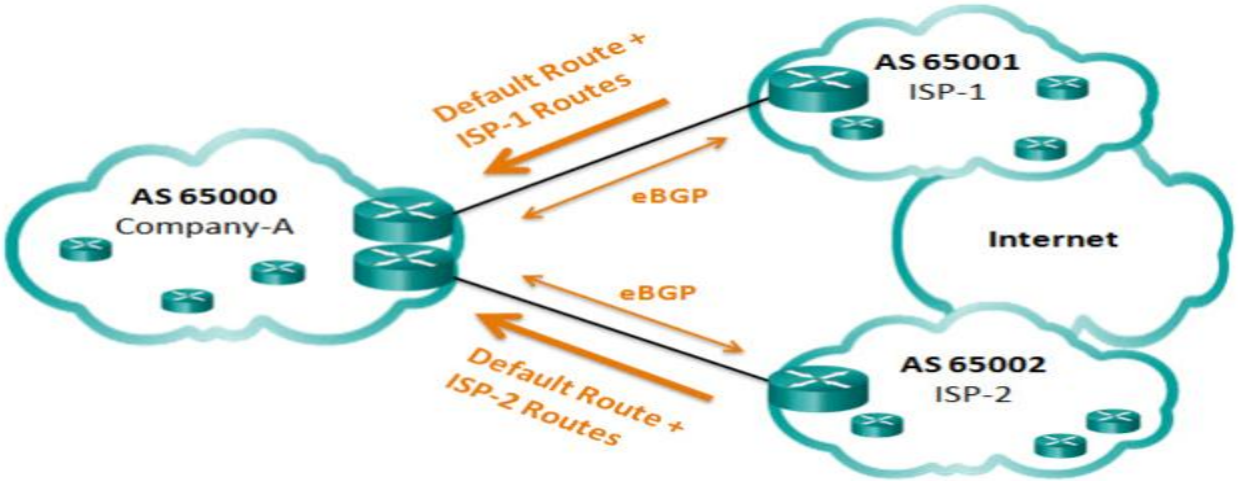
  se puede producir enrutamiento óptimo.

  Este es el método más sencillo.



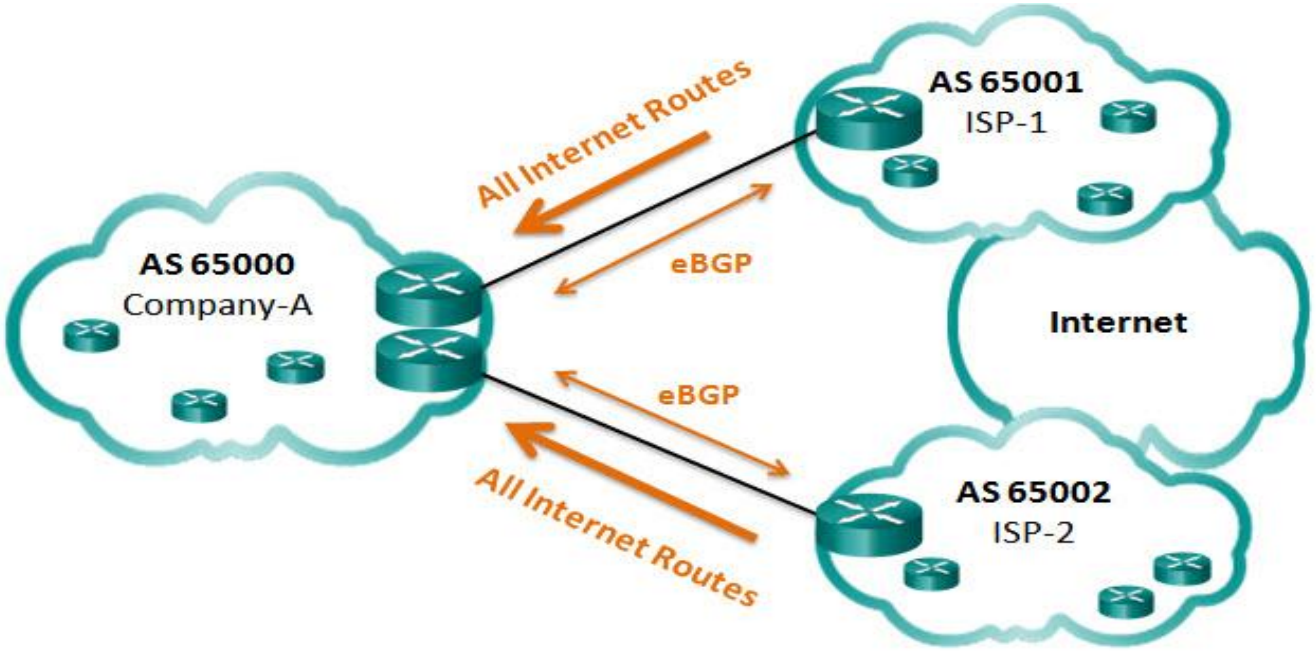
Opciones de BGP

- **Ruta por defecto y Rutas ISP**
- Los ISP anuncia una ruta por defecto ya las redes de otros ISP.
- Permite a la empresa-A que transmita el tráfico hacia el ISP adecuado para redes anunciadas por ese ISP.
- enrutamiento subóptimo puede ocurrir por las redes más allá de los ISP conectados.



Opciones de BGP

- **Todas las rutas de Internet**
- ISP anuncia todas las rutas de Internet a la empresa-A.
- Permite a la empresa para hacer mejores decisiones de encaminamiento para todas las redes.
- Requiere una gran cantidad de recursos en los routers de empresa-a.



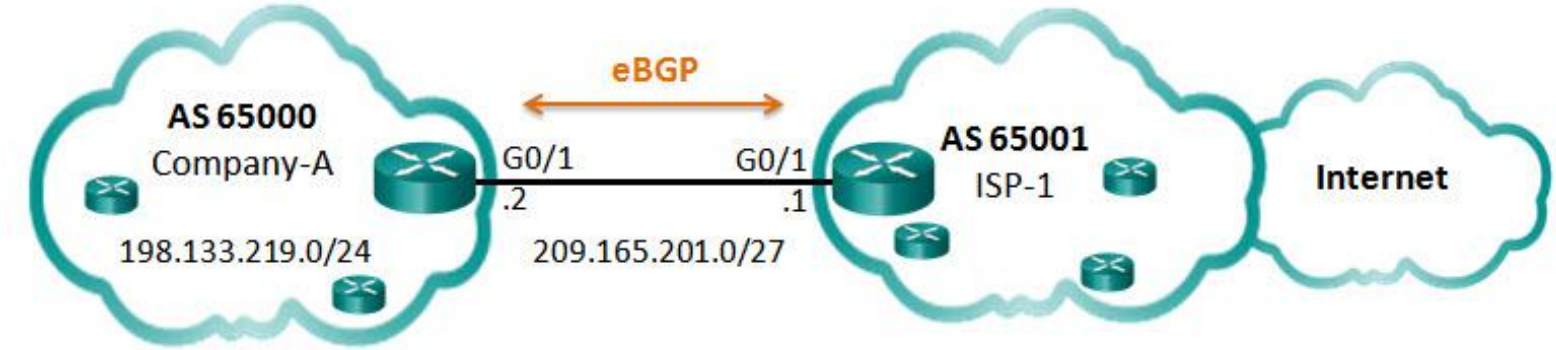
Pasos para configurar eBGP

- Para implementar eBGP en este curso, tendrá que realizar lo siguiente:
- Paso 1: Habilitar el enrutamiento BGP.
- Paso 2: Configurar los vecinos BGP (mirar).
- Paso 3: advertir las redes precedentes de este AS

Command	Description
`Router(config)# router bgp as-number`	Enables a BGP routing process, and places the router in router configuration mode.
`Router(config-router)# neighbor ip-address remote-as as-number`	Specifies a BGP neighbor. The *as-number* is the neighbor's AS number.
`Router(config-router)# network network-address [mask network-mask]`	Advertises a network address to an eBGP neighbor as being originated by this AS. The *network-mask* is the subnet mask of the network.

Ejemplo de configuracion de BGP

- Use eBGP, en la compañia -A con AS 65000 para que advierta la red 198.133.219.0/24 al ISP-1 con AS 65001.
- El ISP-1 advierte la ruta por defecto al eBGP actualizado a la compañia A.




```
Company-A(config)# router bgp 65000
Company-A(config-router)# neighbor 209.165.201.1 remote-as 65001
Company-A(config-router)# network 198.133.219.0 mask 255.255.255.0
```

```
ISP-1(config)# router bgp 65001
ISP-1(config-router)# neighbor 209.165.201.2 remote-as 65000
ISP-1(config-router)# network 0.0.0.0
```

Verificando eBGP

Command	Description
`Router# show ip route`	Verify routes advertised by the BGP neighbor are present in the IPv4 routing table.
`Router# show ip bgp`	Verify that received and advertised IPv4 networks are in the BGP table.
`Router# show ip bgp summary`	Verify IPv4 BGP neighbors and other BGP information.

Verificando eBGP

- **show ip route muestra la salida de la compañia** A
- El código de origen B identifica la ruta que esta utilizando BGP

```
Company-A# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
<output omitted>

Gateway of last resort is 209.165.201.1 to network 0.0.0.0

B*    0.0.0.0/0 [20/0] via 209.165.201.1, 00:36:03
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        198.133.219.0/24 is directly connected, GigabitEthernet0/0
L        198.133.219.1/32 is directly connected, GigabitEthernet0/0
      209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.201.0/27 is directly connected, GigabitEthernet0/1
L        209.165.201.2/32 is directly connected, GigabitEthernet0/1
Company-A#
```

Verificando eBGP

- **show ip bpg muestra la salidoa de la** Compañia A y su table BGP.
- La primera entrada 0.0.0.0 es la ruta por defecto advertida por el ISP-1.
- La segunda entrada 198.133.219.0/24 es la red advertida por la compañia -A por el router del ISP-1.

```
Company-A# show ip bgp
BGP table version is 3, local router ID is 209.165.201.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  0.0.0.0          209.165.201.1            0             0 65001 i
 *>  198.133.219.0/24 0.0.0.0                  0         32768 i
Company-A#
```

Verificando eBGP

- **show ip bgp summary muestra el estado de la conexion** BGP.
- La primera linea muestra la direccion IPV4 usada por el vecino con BGP.
- Última línea es la dirección y el número de AS del vecino BGP.

```
Company-A# show ip bgp summary
BGP router identifier 209.165.201.2, local AS number 65000
BGP table version is 3, main routing table version 3
2 network entries using 288 bytes of memory
2 path entries using 160 bytes of memory
2/2 BGP path/bestpath attribute entries using 320 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 792 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor        V       AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
209.165.201.1   4    65001      66      66        3    0    0 00:56:11            1
Company-A#
```

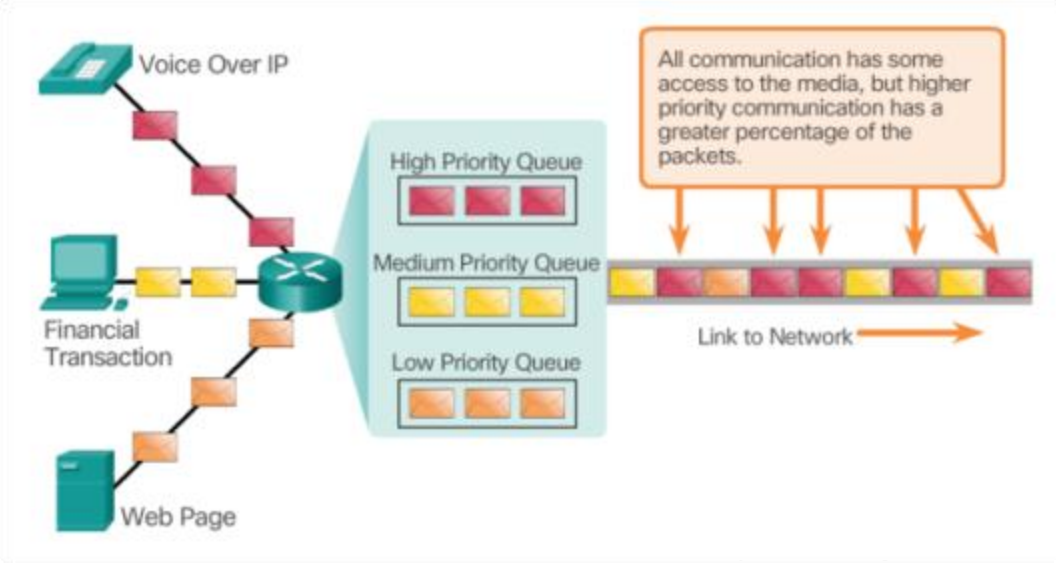
Acerca de QoS

CCNA Routing & Switching 6.0 Bridging

Cisco | Networking Academy®
Mind Wide Open™

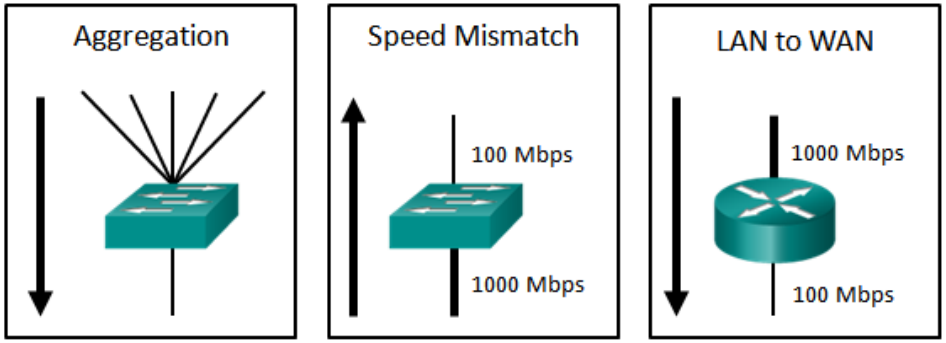
Dar prioridad al tráfico

- Las aplicaciones como transmisiones de vídeo y voz, mayores expectativas sobre la calidad de los servicios prestados.
- La congestión se produce cuando la demanda de ancho de banda es superior a la cantidad disponible.
- Cuando el volumen de tráfico es mayor que lo que puede ser transportado a través de la red, en cola de los paquetes.
- Si el número de paquetes en cola sigue aumentando, las colas de memoria se llenan y se eliminan paquetes.



Bandwidth, Congestion, Delay, and Jitter

- El ancho de banda se mide en el número de bits que pueden transmitirse en un solo segundo, o bits por segundo (bps).
- La congestión provoca retraso, los ejemplos se muestran en la figura.

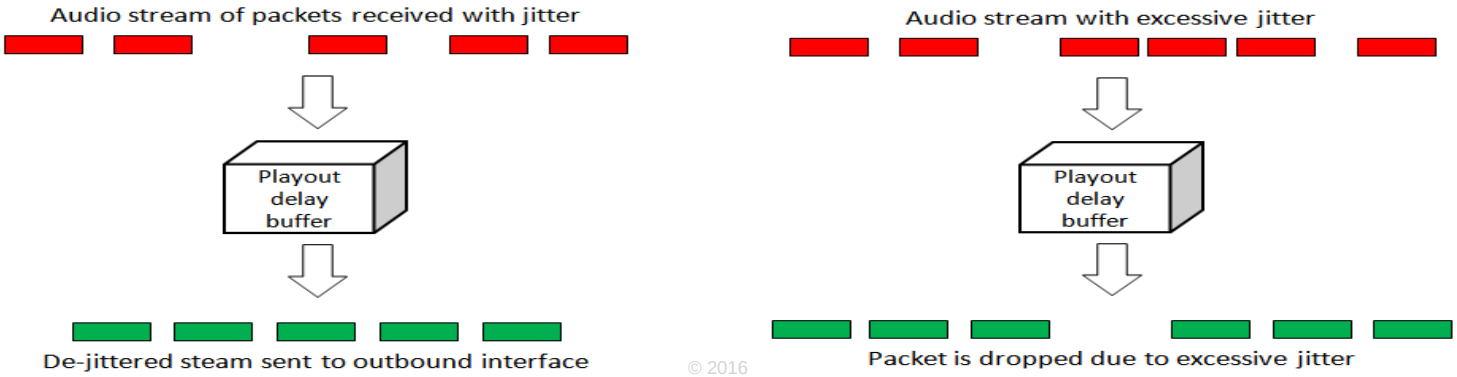


- El retardo o latencia se refiere al tiempo que tarda un paquete en viajar desde el origen al destino.

Delay	Description
Code delay	The fixed amount of time it takes to compress data at the source before transmitting to the first internetworking device, usually a switch.
Packetization delay	The fixed time it takes to encapsulate a packet with all the necessary header information.
Queuing delay	The variable amount of time a frame or packet waits to be transmitted on the link.
Serialization delay	The fixed amount of time it takes to transmit a frame from the NIC to the wire.
Propagation delay	The variable amount of time it takes for the frame to traverse the links between the source and destination.
De-jitter delay	The fixed amount of time it takes to buffer a flow of packets and then send them out in evenly spaced intervals.

Perdida de paquetes

- Cuando se produce la congestión, los routers y switch comienzan a botar los paquetes.
- Cuando un router recibe un Protocolo en Tiempo Real (RTP) flujo de audio para (VoIP), debe compensar la fluctuación de fase.
- El buffer de retardo en reproducción debe amortiguar estos paquetes y luego reproducirlos en un flujo constante.
- Si la fluctuación de fase es tan grande que hace que los paquetes que se reciban fuera del alcance de este, los paquetes fuera de la gama se descartan y los abandonos se escuchan en el audio, como se muestra en la figura de la derecha.



Tendencias del tráfico de red

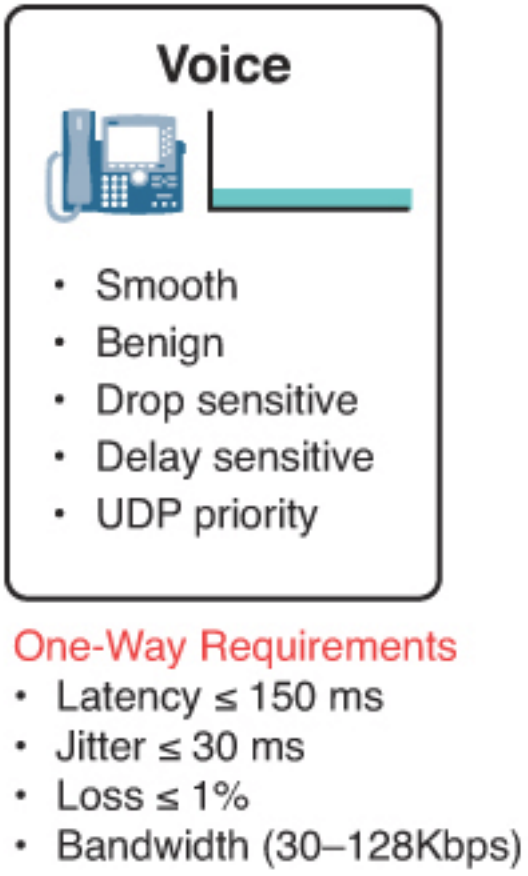
- Década de 2000, el tráfico IP eran de voz y datos.
- Recientemente, el tráfico de vídeo es más importante para las comunicaciones de negocios y operaciones.
- De acuerdo con el Índice de Redes Cisco Virtual (VNI):
- El tráfico de video representó el 67% de todo el tráfico en 2014.

- En 2019, el vídeo representará el 80% de todo el tráfico.

- El tráfico de video móvil se incrementará con el 600% de 113.672TB a 768.334 TB.

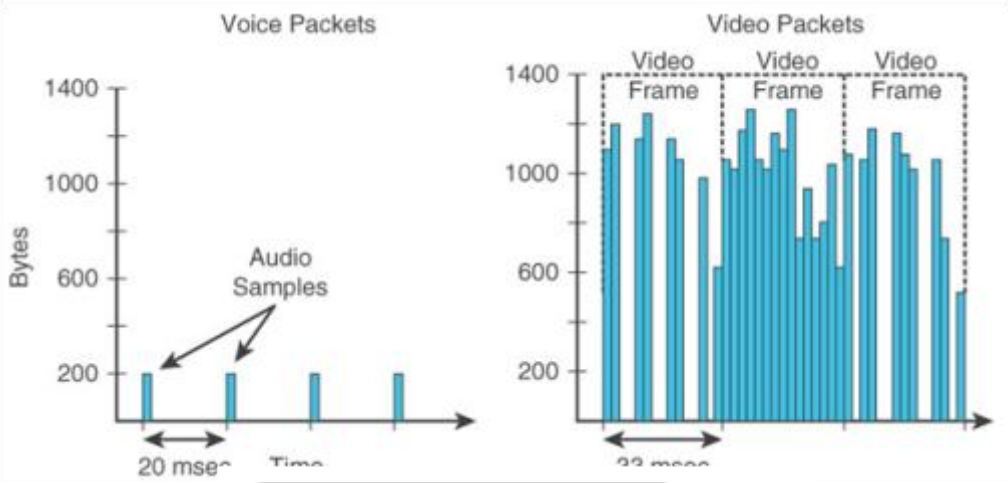
Voz

- El tráfico de voz es predecible y suave.
- Sin embargo, la voz es muy sensible a los retrasos y la pérdida de paquetes y no puede ser retransmitido en caso de pérdida.
- El tráfico de voz debe recibir una prioridad más alta UDP.
- Voz puede tolerar una cierta cantidad de latencia, jitter y pérdida, y no afecta a su reenvio de manera notable.



Video

- El tráfico de video tiende a ser impredecible, inconsistente, y en ráfagas.
- El video es menos resistente a la pérdida y tiene un mayor volumen de datos por paquetes.
- Similar a voz, además el vídeo puede tolerar una cierta cantidad de latencia, fluctuación de fase, y la pérdida sin afectación notable



Video

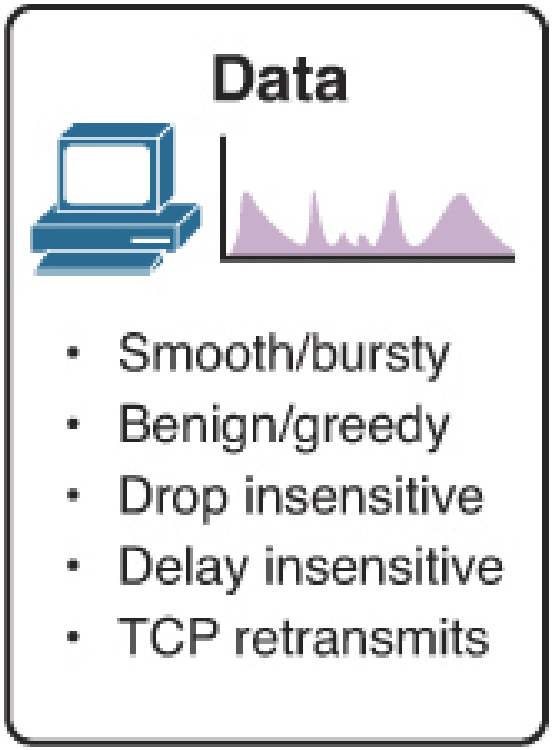
- Bursty
- Greedy
- Drop sensitive
- Delay sensitive
- UDP priority

One-Way Requirements

- Latency ≤ 200-400 ms
- Jitter ≤ 30-50 ms
- Loss ≤ 0.1-1%
- Bandwidth (384Kbps–20 + Mbps)

Los datos

- El uso de los datos que no tienen tolerancia a la pérdida de datos, como correo electrónico y páginas web, utilizan TCP para garantizar que, si se pierden paquetes en tránsito, serán re-enviados.
- El tráfico de datos puede ser pleno y en ráfagas.
- Algunas aplicaciones TCP pueden ser consumir una gran parte de capacidad de red.
- FTP consumirá tanto ancho de banda como se puede conseguir cuando se descarga un archivo de gran tamaño, como una película o un juego.



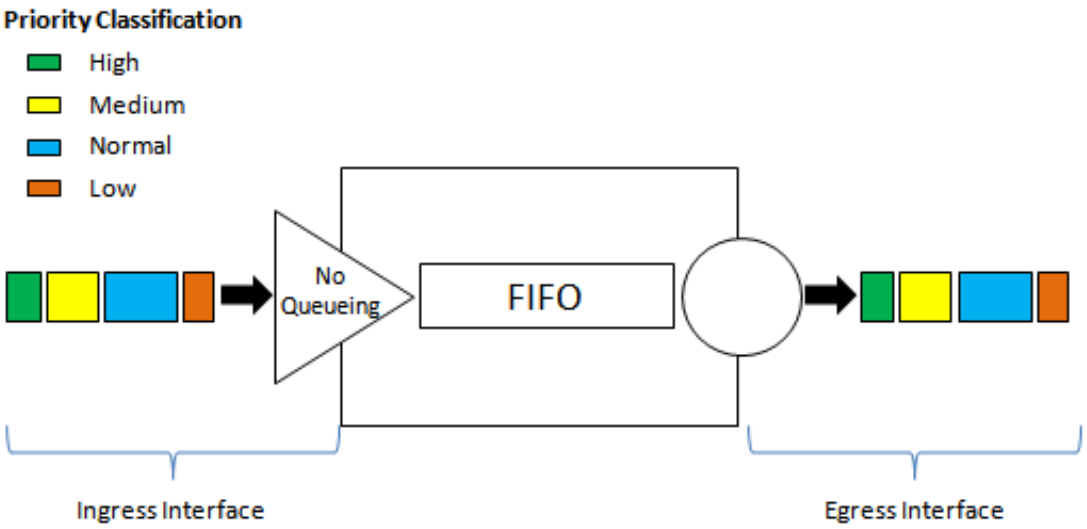
Los datos

- El tráfico de datos es relativamente insensible a perdidas y retrasos en comparación con voz y vídeo
- El administrador de la red debe tener en cuenta la calidad de la experiencia del usuario.
- Dos factores principales se debe preguntar sobre el flujo de tráfico de datos:
- ¿Los datos provienen de una aplicación interactiva?
- Es fundamental y critico los datos?

Factor	Mission Critical	Not Mission Critical
Interactive	Prioritize for the lowest delay of all data traffic and strive for a 1 to 2 response time.	Applications could benefit from lower delay.
Not interactive	Delay can vary greatly as long as the necessary minimum bandwidth is supplied.	Gets any leftover bandwidth after all voice, video, and other data application needs are met.

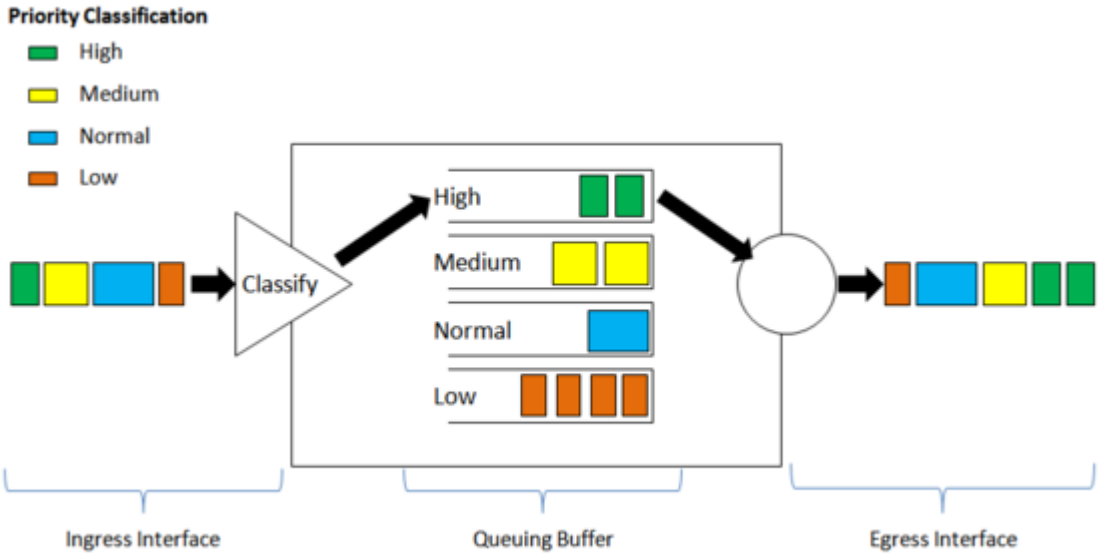
Algoritmos de encolamiento

primero en entrar primero en salir (FIFO)



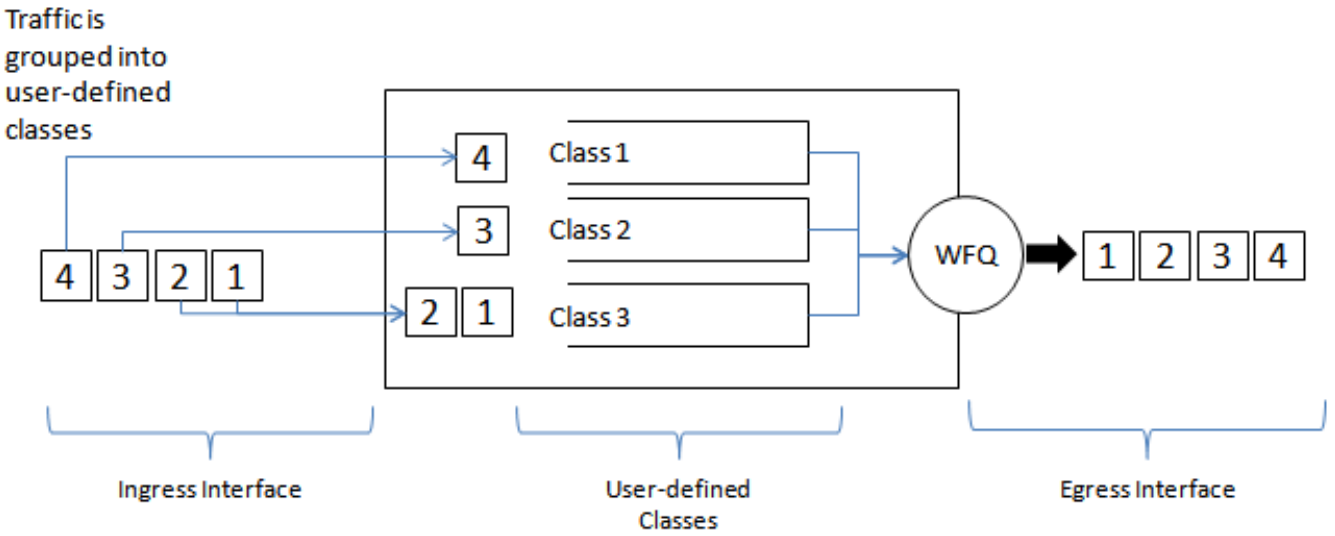
- FIFO implica la puesta en cola de amortiguación y el reenvío de paquetes en el orden de llegada.
- FIFO no reconoce prioridad o clases de tráfico.
- El tráfico se envía en el orden que se recibe.
- FIFO, que es el método más rápido de puesta en cola, es eficaz para grandes enlaces que tienen poco de retardo y la congestión mínima.

Encolamiento justo y ponderado (WFQ)



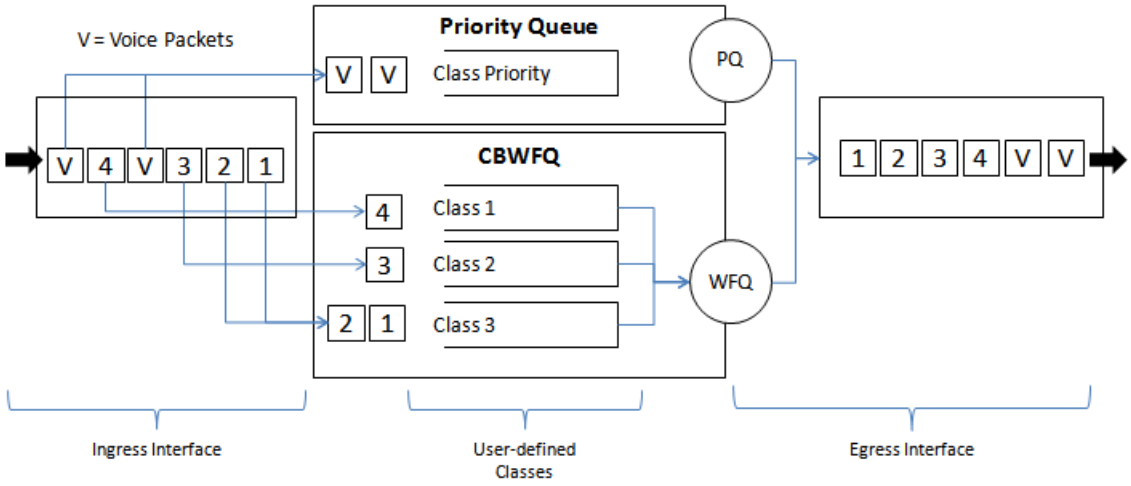
- WFQ es un método de programación automatizada que proporciona la asignación de ancho de banda justo para todo el tráfico de red.
- WFQ permite dar de baja el volumen, el tráfico interactivo, como Telnet y voz, y prioridad sobre el tráfico de alto volumen, como FTP.
- WFQ clasifica el tráfico en diferentes flujos basados en la cabecera del paquete
- flujos de tráfico con bajo ancho de banda reciban un servicio preferente.

Encolamiento justo y ponderado Basado en clases(CBWFQ)



- CBWFQ amplía la funcionalidad WFQ proporciona apoyo a las clases de tráfico definidas por el usuario.
- Una cola FIFO está reservado para cada clase, y el tráfico que pertenece a una clase está dirigida a la cola para esa clase.
- Para la caracterización de una clase, se le asigna el ancho de banda, el peso, y el límite máximo de paquete.
- El ancho de banda asignado a una clase es el ancho de banda garantizado entregado a la clase durante la congestión.

Baja latencia de encolamiento (LLQ)



- LLQ tiene la característica de prioridad de cola (PQ) para CBWFQ.
- Con LLQ, los datos sensibles al retardo se envía primero, antes que los paquetes en otras colas sean tratados.
- LLQ permite que los datos sensibles al retardo, como voz sean enviados primero (antes que los paquetes en otras colas), dando a los datos sensibles al retardo tratamiento preferente sobre el resto del tráfico.
- Aunque es posible poner en cola los distintos tipos de tráfico en tiempo real para la cola de prioridad estricta, se recomienda que sólo el tráfico de voz se dirija a él.

Selección de un modelo de política de QoS adecuada

- Hay tres modelos para la aplicación de QoS.

Model	Description
Best-effort model	• Not really an implementation as QoS is not explicitly configured. • Use when QoS is not required.
Integrated services (IntServ)	• Provides very high QoS to IP packets with guaranteed delivery. • It defines a signaling process for applications to signal to the network that they require special QoS for a period and that bandwidth should be reserved. • However, IntServ can severely limit the scalability of a network.
Differentiated services (DiffServ)	• Provides high scalability and flexibility in implementing QoS. • Network devices recognize traffic classes and provide different levels of QoS to different traffic classes.

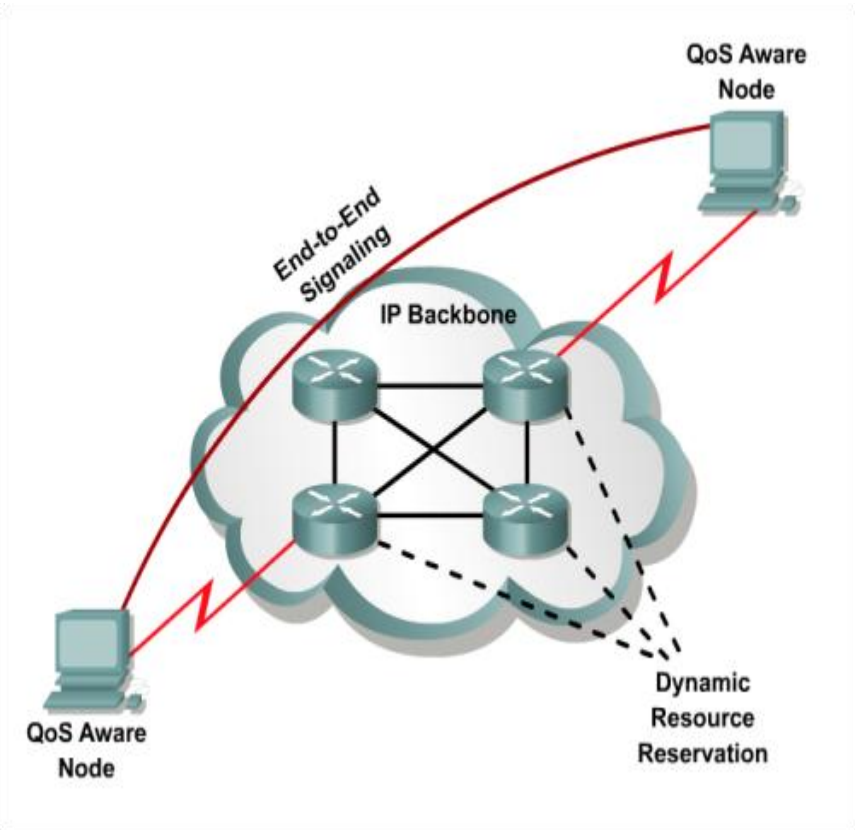
Mejor Esfuerzo (Best Effort)

- la entrega de paquetes de mejor esfuerzo no proporciona garantías.
- Adecuada para la mayoría de los propósitos.
- Ventajas y desventajas de Mejor Esfuerzo-modelo se muestran en la tabla.

Benefits	Drawbacks
• The model is the most scalable. • Scalability is only limited by bandwidth limits, in which case all traffic is equally affected. • No special QoS mechanisms are required. • Therefore it is the easiest and quickest model to deploy.	• There are no guarantees of delivery. • Packets will arrive whenever they can and in any order possible, if they arrive at all. • No packets have preferential treatment. • Critical data is treated the same as casual e-mail is treated.

Servicios integrados

- IntServ modelo de múltiples servicios que pueden acomodar múltiples requerimientos de QoS.
- IntServ ofrece una manera de ofrecer la QoS de extremo a extremo que las aplicaciones en tiempo real requieren explícitamente mediante la gestión de los recursos de red para proporcionar QoS a los flujos de paquetes específicos del usuario, a veces llamado microflujos.
- IntServ utiliza un enfoque orientado a la conexión heredado de diseño de la red de telefonía.



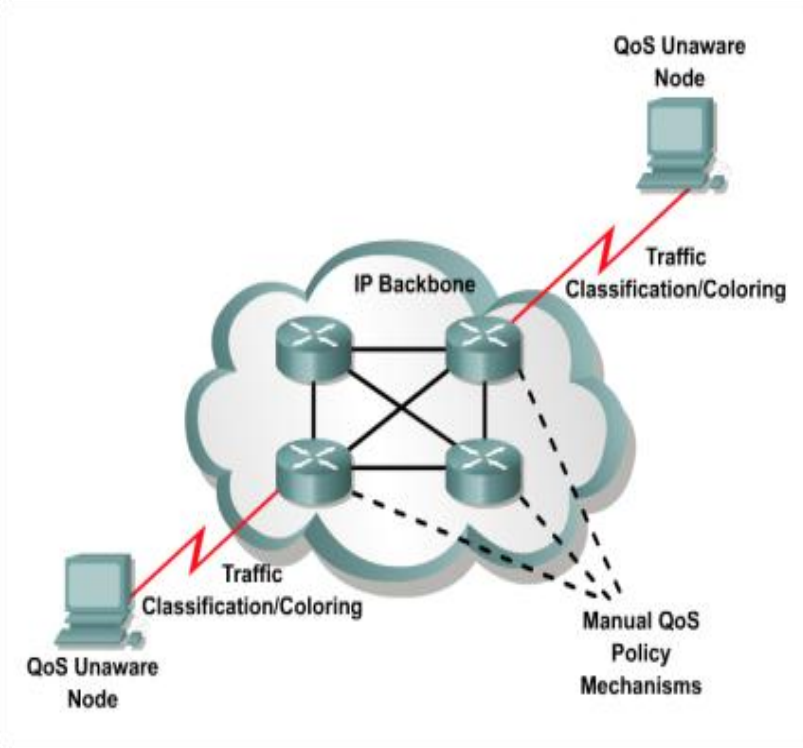
Servicios integrados

- La aplicación solicita un tipo específico de servicio de la red antes de enviar datos.
- La aplicación informa a la red de su perfil de tráfico y solicita un tipo particular de servicio que puede abarcar sus requisitos de ancho de banda y de retardo.
- IntServ usa el Protocolo de reserva de recursos (RSVP) para señalar las necesidades de QoS de tráfico de una aplicación a lo largo de los dispositivos de la ruta de extremo a extremo a través de la red.

Benefits	Drawbacks
• Explicit end-to-end resource admission control • Per-request policy admission control (authorization object, policy object) • Signaling of dynamic port numbers such as H.323	• Resource intensive due to the stateful architecture requirement for continuous signaling. • Flow-based approach not scalable to large implementations such as the Internet.

Servicios diferenciados

- Los servicios diferenciados (DiffServ) especifica un mecanismo simple y escalable para la clasificación y la gestión de tráfico de la red y proporcionar garantías de QoS en redes IP modernas.
- DiffServ no es una estrategia de extremo a extremo QoS.
- DiffServ QoS enfoque más escalable.
- A diferencia de IntServ DiffServ no utiliza la señalización.
- En su lugar, DiffServ funciona en el modelo aprovisionado-QoS, donde los elementos de red están configurados para dar servicio a múltiples clases de tráfico, cada uno con diferentes requisitos de QoS.

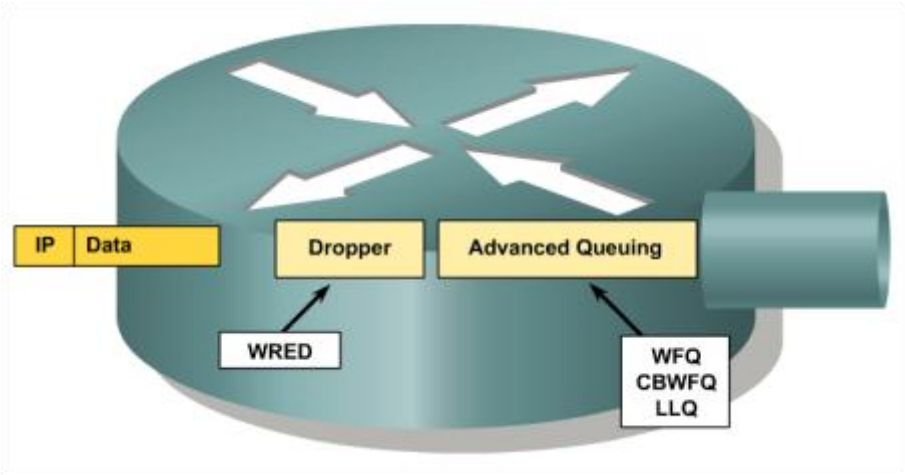


Servicios diferenciados

- DiffServ impone y aplica mecanismos de QoS sobre una base salto a salto, y aplica uniformemente significado global para cada clase de tráfico para proporcionar la flexibilidad y la escalabilidad.
- DiffServ divide el tráfico de red en clases basándose en los requisitos empresariales.
- Cada una de las clases a continuación, se le puede asignar un nivel diferente de servicio.
- A medida que los paquetes atraviesen una red, cada uno de los dispositivos de red identifica la clase y los servicios de paquetes del paquete de acuerdo a esa clase.
- Una red moderna utiliza principalmente el modelo DiffServ, aunque IntServ y RSVP es a veces co-desplegado.

Benefits	Drawbacks
• Highly scalable • Provides many different levels of quality	• No absolute guarantee of service quality • Requires a set of complex mechanisms to work in concert throughout the network

Cómo evitar la pérdida de paquetes



- La pérdida de paquetes es generalmente el resultado de la congestión en una interfaz.
- segmentos TCP que causan sesiones TCP para reducir tamaños de la ventana.
- Estos enfoques pueden impedir la perdida en aplicaciones sensibles:
- 1. Aumentar la capacidad del enlace para aliviar o prevenir la congestión.
- 2. Garantizar suficiente ancho de banda y aumentar el espacio de memoria intermedia para dar cabida a las ráfagas de tráfico de los flujos frágiles.
- 3. Evitar la congestión dejando caer los paquetes de menor prioridad antes de que ocurra la congestión.

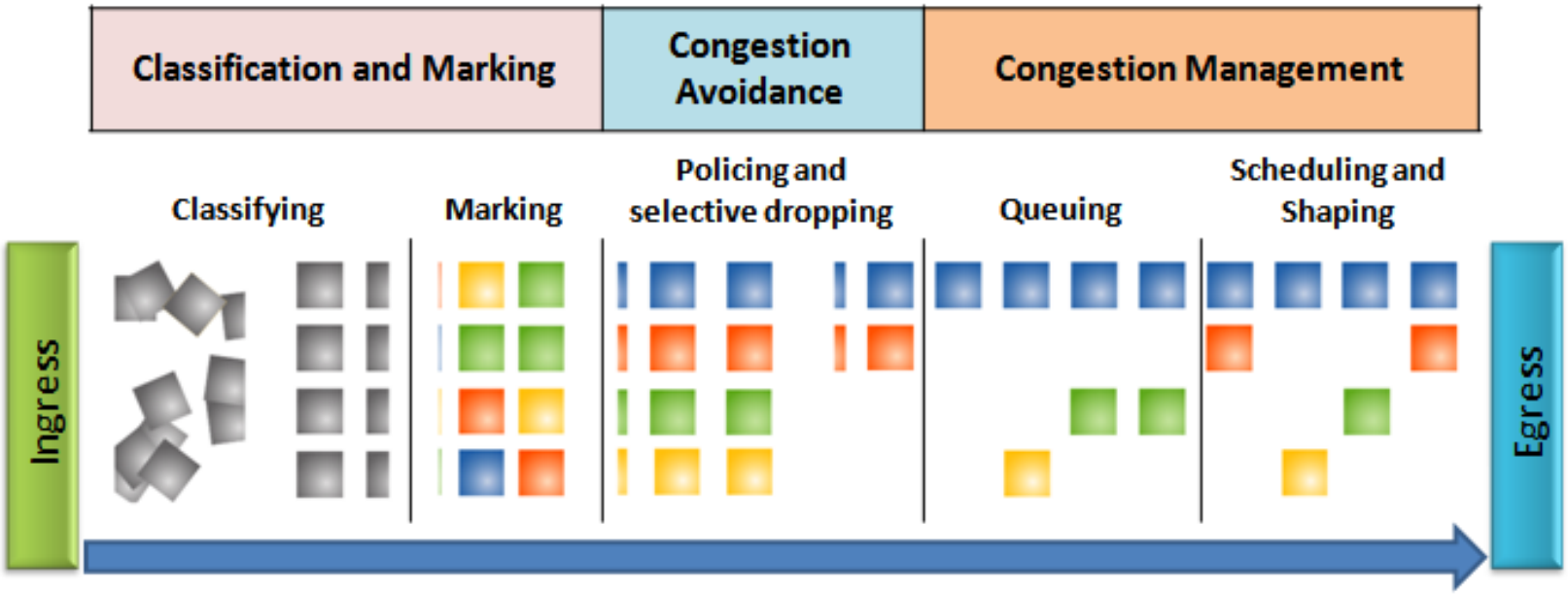
Herramientas de QoS

- Tres categorías de herramientas de calidad de servicio:

QoS Tools	Description
Classification and marking tools	• Sessions, or flows, are analyzed to determine what traffic class they belong to • Once determined, the packets are marked.
Congestion avoidance tools	• Traffic classes are allotted portions of network resources as defined by the QoS policy. • The QoS policy also identifies how some traffic may be selectively dropped, delayed, or re-marked to avoid congestion. • The primary congestion avoidance tool is WRED and is used to regulate TCP data traffic in a bandwidth-efficient manner before tail drops caused by queue overflows occur.
Congestion management tools	• When traffic exceeds available network resources, traffic is queued to await availability of resources. • Common Cisco IOS-based congestion management tools include CBWFQ and LLQ algorithms.

Herramientas de QoS

- Paquetes de ingreso (cuadrados grises) se clasifican y su respectiva cabecera IP se marca (cuadros de colores).
- Para evitar la congestión, los paquetes se asignan entonces los recursos basados en políticas definidas.
- Los paquetes entonces en cola y se envía a cabo la interfaz de salida en función de sus QoS definidos que dan forma y condición a la política.



Operacion de QoS y como trabajan sus herramientas

Clasificacion y marcacion

Seleccione la cola y la perdida de paquetes

Operacion despues de la cola

Clasificación y Marcado

- Antes de que un paquete pueda tener una política de QoS, el paquete tiene que ser clasificado.
- La Clasificación determina qué clase de paquete de tráfico.
- Sólo después de que el tráfico se identifica positivamente se pueden aplicar políticas a la misma.
- Métodos de clasificación de los flujos de tráfico en la Capa 2 y 3 incluyen el uso de interfaces, ACL, y mapas de clase.
- Estamos agregando un valor a la cabecera del paquete marcado.
- Dispositivos que reciben el paquete miran este campo para ver si coincide con una política definida.
- El Marcado debería realizarse lo más cerca posible del dispositivo fuente como sea posible.
- Esto establece el límite de confianza.

Clasificación y Marcado

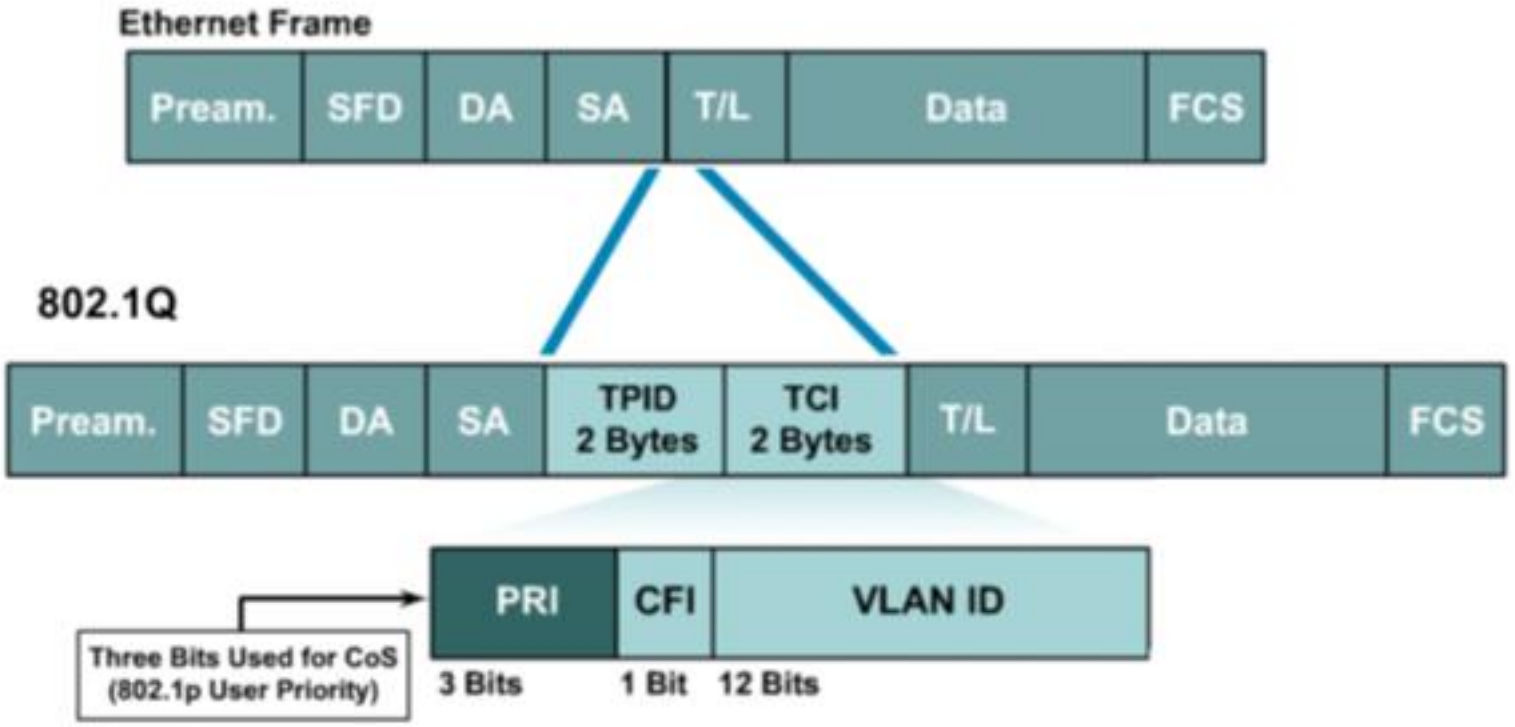
- El tráfico marcado por lo general depende de la tecnología.

QoS Tools	Layer	Marking Field	Width in Bits
Ethernet (802.1Q, 802.1p)	2	Class of Service (CoS)	3
802.11 (Wi-Fi)	2	Wi-Fi Traffic Identifier (TID)	3
MPLS	2	Experimental (EXP)	3
IPv4 and IPv6	3	IP Precedence	3
IPv4 and IPv6	3	Differentiated Services Code Point (DSCP)	6

- La decisión de si se debe marcar el tráfico en las Capas 2 o 3 o ambos, no es trivial y se debe hacer después de considerar los siguientes puntos:
- El marcado en la Capa 2 se puede llevar a cabo para el tráfico no-IP.
- El marcado en la Capa 2 es la única opción de calidad de servicio disponible para swtich que no son "conscientes de IP"
- En marcado en la Capa 3 llevará información de QoS de extremo a extremo.

Marcado en la capa 2

- 802.1Q estándar es una especificación IEEE para la implementación de VLAN de capa 2 en redes de conmutación.
- Dos campos se insertan en la trama Ethernet que sigue al campo de dirección de origen.



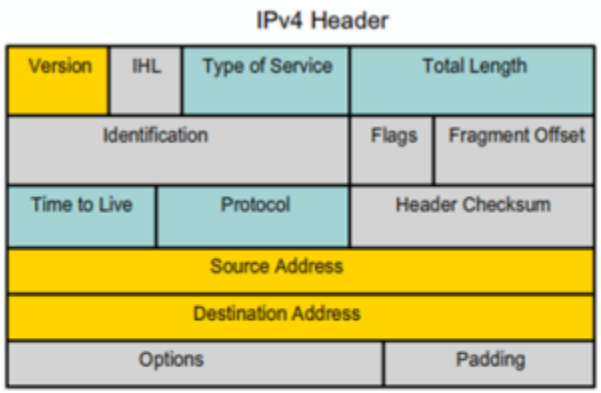
Marcado en la capa 2

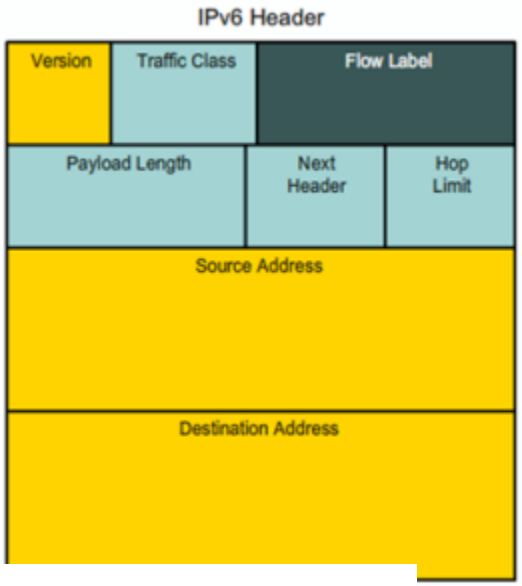
- identificador de protocolo Tag (TPID) está fijado actualmente y se le asigna el valor 0x8100.
- La información de control de etiqueta (TCI) contiene 3 bits de PRI (Prioridad) que identifica la clase de marcas de servicio (CoS).
- El Consejo de Estado de marcaje permite una trama de Ethernet de Capa 2 que se marcará con ocho niveles de prioridad (valores 0-7).

Value	Description
7	Reserved
6	Reserved
5	Voice bearer (voice traffic)
4	Videoconferencing
3	Call Signaling
2	High-Priority Data
1	Medium-Priority Data
0	Best-Effort Data

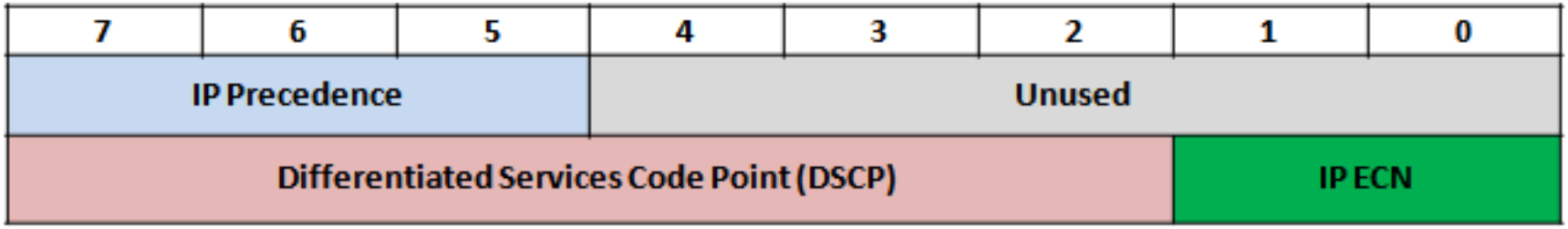
Marcado en la capa 3

- IPv4 e IPv6 especifica un campo de 8 bits en sus cabeceras de los paquetes para marcar paquetes
- IPv4: "Tipo de servicio"
- IPv6 "Clase de tráfico"





Tipo de servicio y la Clase de tráfico contienen



Marcado en la capa 3

- Los primeros bits de orden 3 significativa o se refiere como el campo de precedencia IP.
- Los 8 bits proporciona un total de ocho posibles clases de servicio.

Value	Description
7	Network
6	Internet
5	Critical
4	Flash-override
3	Flash
2	Immediate
1	Priority
0	Routine

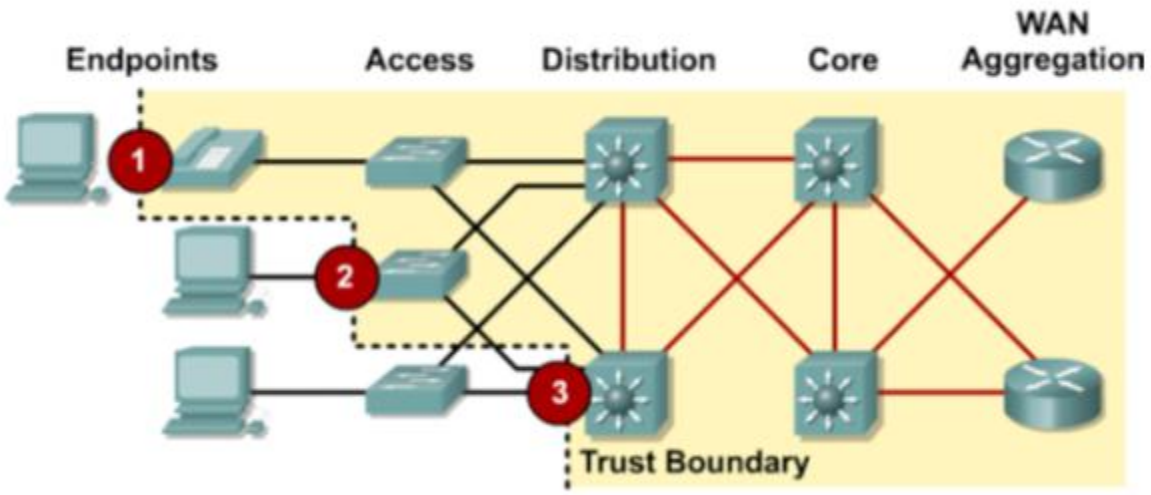
Marcado en la capa 3

- Con el modelo DiffServ, el paquete es marcado con 6 bits que se hace referencia como los bits de código de DiffServ Point (DSCP). Seis bits ofrece un máximo de 64 posibles clases de servicio.
- Los routers con Diffserv implementan comportamientos por salto (PHB), que definen las propiedades de envío de paquetes asociados con una clase de tráfico.
- Hay cuatro categorías de PBH:

PHB Category	Description
Default	• Used for best-effort service. • Left-most DSCP bits equal **000**xxx
Expedited Forwarding (EF)	• Used for low-delay service providing a low-loss, low-latency, low-jitter, and assured bandwidth service for applications such as voice and video. • Left-most DSCP bits equal **101**xxx
Assured Forwarding (AF)	• Used for guaranteed bandwidth service. • It defines 4 sub-classes (AF1, AF2, AF3, and AF4). • Left-most DSCP bits equal **001**xxx, **010**xxx, **011**xxx, or **100**xxx
Call Selector	• Used for backward compatibility with non-DiffServ-compliant devices • Bits 2 to 4 of DSCP equal xxx**000**.

los límites de confianza

- El tráfico debe ser clasificado y marcado lo mas cerca de su fuente que sea técnica y administrativamente factible. para definir el límite de confianza.



Los criterios de valoración de confianza tienen la capacidad y la inteligencia para marcar el tráfico de aplicaciones a la capa correspondiente 2 cos/Capa 3. Los valores de DSCP.

- Los extremos seguros pueden tener tráfico marcado en el switch.
- El tráfico también se puede marcar en la Capa 3 switches / routers.

los límites de confianza

- Re-marcar el tráfico es normalmente necesario, con esta remarcación los valores de calidad de servicio y de IP precedencia o valores DSCP.

Application	L3 Classification			L2
	IPP	PHB	DSCP	CoS
Routing	6	CS6	48	6
Voice	5	EF	46	5
Video Conferencing	4	AF41	34	4
Streaming Video	4	CS4	32	4
Mission-Critical Data	3	AF31	26	3
Call Signaling	3	CS3	24	3
Transactional Data	2	AF21	18	2
Network Management	2	CS2	16	2
Bulk Data	1	AF11	10	1
Best Effort	0	0	0	0
Scavenger	1	CS1	8	1

Evitar la congestión

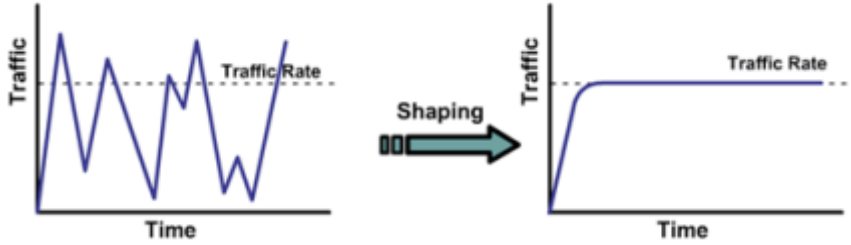
- Las herramientas para evitar la congestión son más simples. Siguen de cerca las cargas de tráfico de red en un esfuerzo para anticipar y evitar la congestión en la red de interconexión de redes comunes y los cuellos de botella antes de la congestión se convierte en un problema.

- Estas técnicas proporcionan un tratamiento preferencial para el tráfico premium (prioridad) cuando hay congestión, mientras que al mismo tiempo maximizar el rendimiento de la red y el uso de la capacidad y reducir al mínimo la pérdida de paquetes y el retardo.

- El algoritmo WRED permite evitar la congestión en interfaces de red, proporcionando gestión de memoria intermedia y permitir el tráfico TCP para disminuir o desacelerar, antes de que se agoten las memorias intermedias.

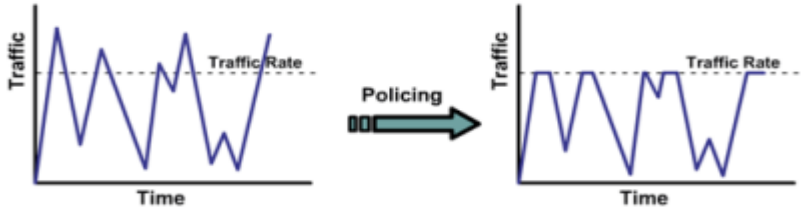
Conformación y Vigilancia (Shaping and Policing)

- la conformación y las políticas de tráfico son dos mecanismos proporcionados por QoS para evitar la congestión.
- La conformación retiene el exceso de paquetes en una cola y después programa el exceso para su posterior transmisión a través de incrementos de tiempo. El resultado es una tasa de salida de paquetes de suavizado.



Directivas de tráfico se propaga en ráfagas.

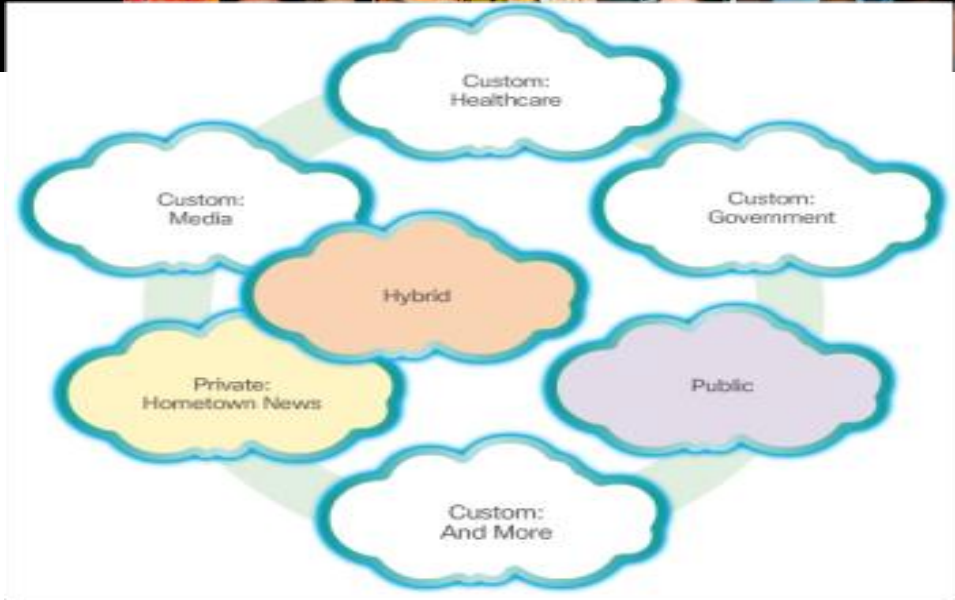
- Cuando la tasa de tráfico alcanza la tasa máxima, se deja caer el exceso de tráfico (o remarcó). El resultado es una tasa de salida asi:



servicios en la nube

- Están disponibles en una variedad de opciones, adaptadas a las necesidades del cliente.
- Los tres principales servicios de computación en la nube definidos por el Instituto Nacional de Estándares y Tecnología (NIST):
- **Software como Servicio (SaaS):** El ISP de la nube es responsable de acceso a los servicios, como el e-mail, la comunicación y de office 365 que se entregan a través de Internet. Los usuarios sólo proporcionan sus datos.
- **Plataforma como servicio (PaaS):** El ISP de la nube es responsable del acceso a las herramientas y servicios de desarrollo utilizados para entregar las aplicaciones.
- **Infraestructura como Servicio (IaaS):** El ISP de la nube es responsable del acceso a los equipos de red, servicios de red virtualizados, y el apoyo a la infraestructura de red.
- los ISP en la nube han extendido este modelo también para proporcionar soporte de TI para cada uno de los servicios en la nube (ITaaS).

Modelos de la nube



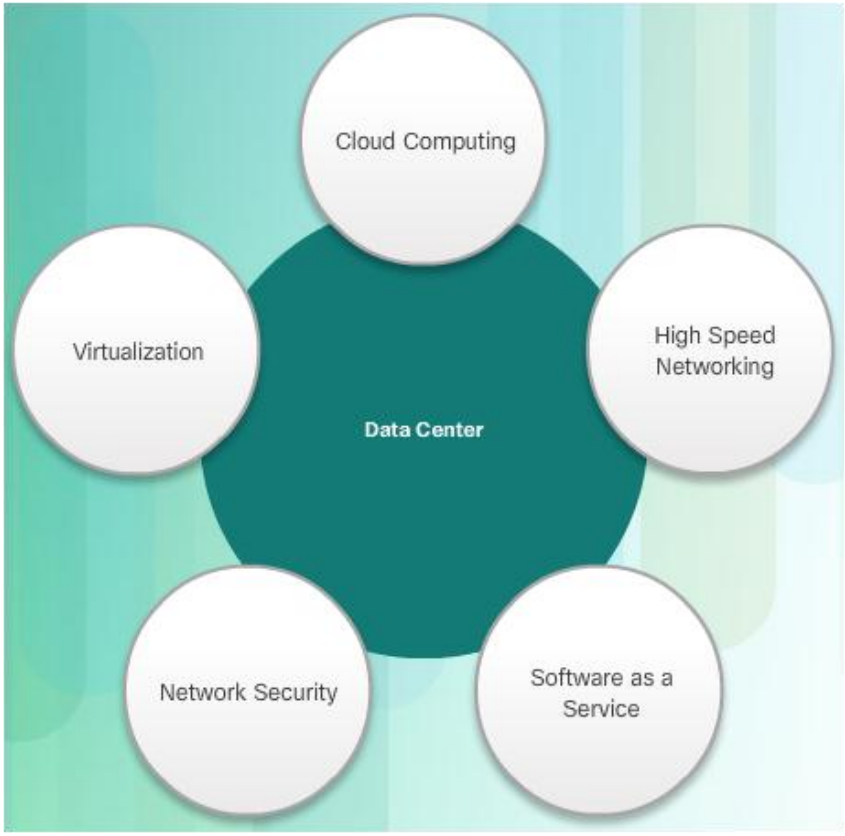
- **Las nubes públicas**: aplicaciones basadas en la nube y los servicios ofrecidos en una nube pública se ponen a disposición de la población en general. Los servicios pueden ser libres o se pongan en un modelo de pago por uso.

- **Las nubes privadas:** las aplicaciones basadas en la nube y los servicios ofrecidos en una nube privada se destinan a una organización o entidad específica, como por ejemplo el gobierno. puede ser administrado por una organización externa con la seguridad de acceso estricto.

- **Las nubes híbridas:** se compone de dos o más nubes (personalizados parte, y parte pública), donde cada parte sigue siendo un objeto distintivo. Ambos están conectados mediante una única arquitectura ..
- **Nubes personalizados**: Son construidas para satisfacer las necesidades de una industria específica, como la salud o el medio. pueden ser privados o públicos.

Computación en la nube vs Centro de Datos

- **centro de datos:** un almacenamiento de datos y la instalación de procesamiento dirigido por un departamento de TI en la empresa o fuera de las instalaciones arrendadas.
- **La computación en nube:** un servicio fuera de las instalaciones que ofrece acceso bajo demanda a un conjunto compartido de recursos informáticos configurables. Estos recursos se pueden aprovisionar rápidamente y puestos en libertad con mínimo esfuerzo de gestión.



Computacion en la nube vs virtualizacion

- Los términos "Cloud computing" y "virtualización" se usan indistintamente; sin embargo, significan cosas diferentes.
- La computación en nube separa la aplicación desde el hardware.
- La virtualización separa el sistema operativo del hardware.
- La virtualización es el fundamento de la computación en nube.
- Varios ISP ofrecen servicios en la nube virtual que puede aprovisionar servidores dinámicamente según sea necesario.

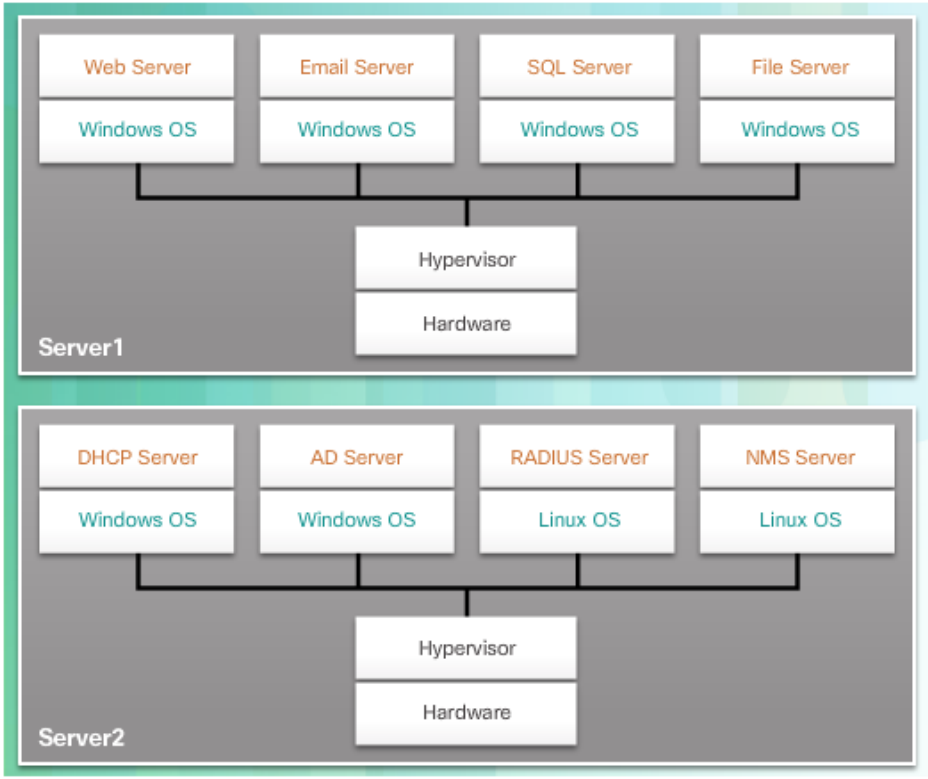
Servidores Dedicados

- Históricamente, los servidores de la empresa consistía en un sistema operativo de servidor (OS), como Windows Server o Servidor Linux, instalado en un hardware específico.

El principal problema de esta configuración es que cuando un componente falla, el servicio que es proporcionado por este servidor no está disponible. Esto se conoce como un único punto de fallo.

La virtualización del servidor

- La virtualización de servidores se aprovecha de los recursos ociosos y consolida el número de servidores necesarios.
- Permite a múltiples sistemas operativos que existen en una única plataforma de hardware.

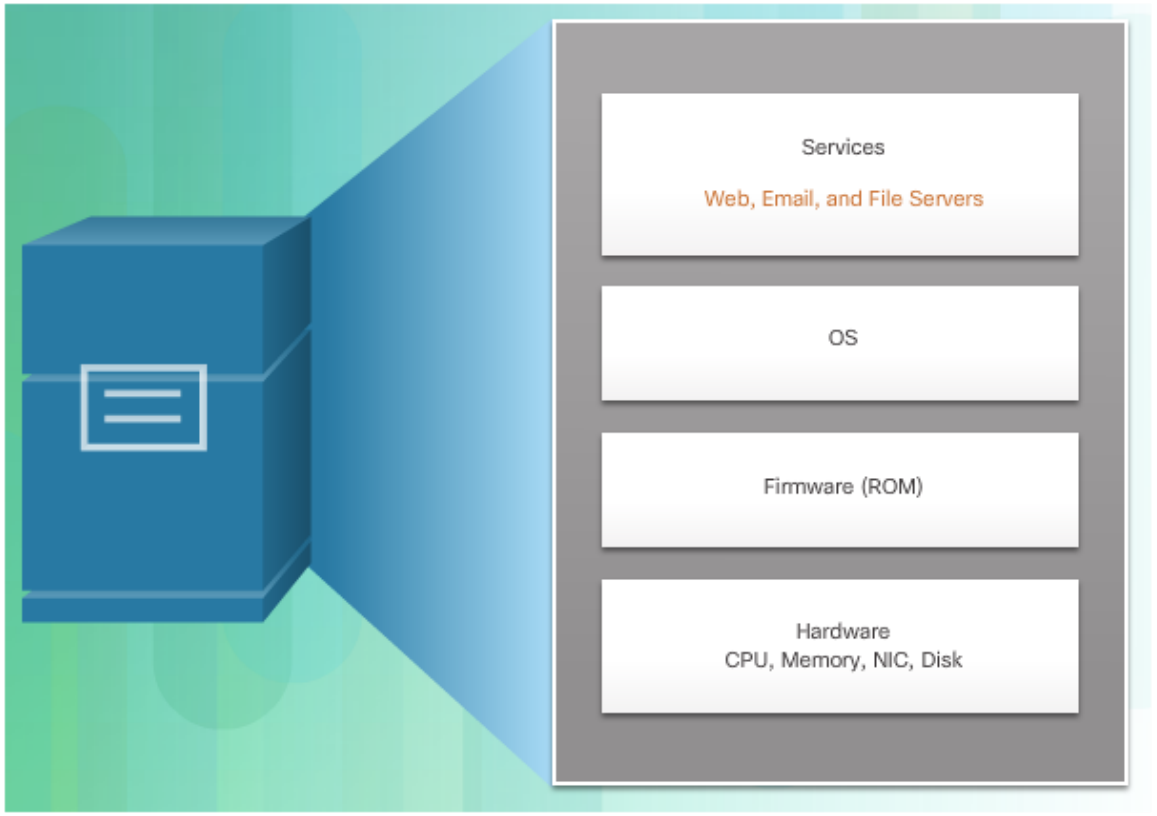


Ventajas de la virtualizacion

- Una de las principales ventajas de la virtualización es que se reduce el costo general:
- Se requiere menos equipo
- Se consume menos energía
- Se requiere menos espacio
- Prototipos más fácil
- Más rápido aprovisionamiento de servidores
- El aumento de la actividad del servidor
- Mejora la recuperación de desastres
- Soporte legal

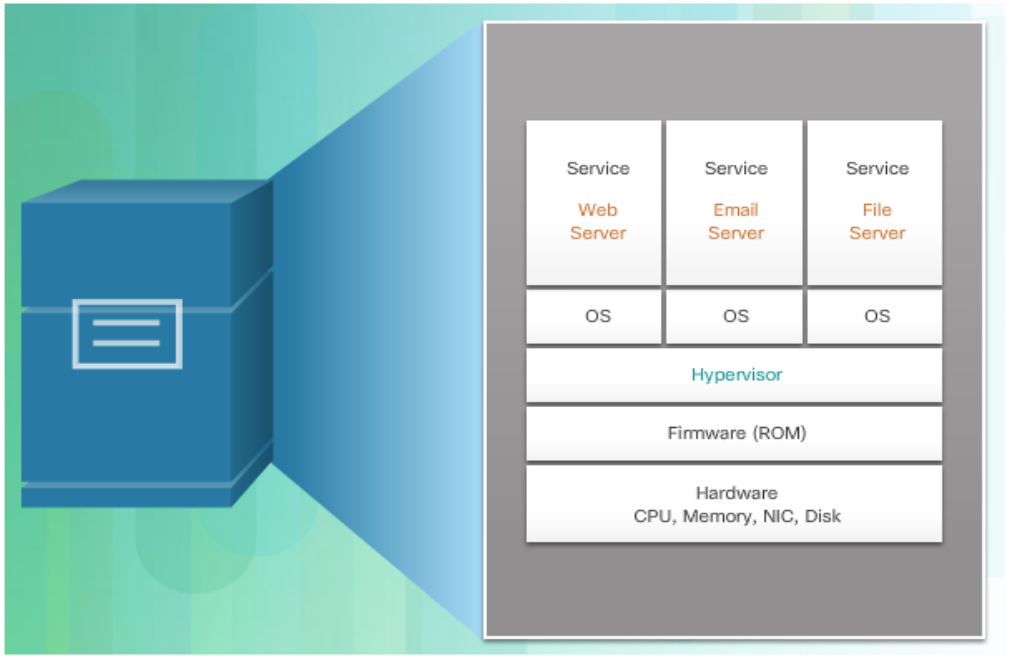
Las capas de abstracción

- Un sistema informático se compone de las siguientes capas de abstracción:
- Servicios
- OS
- firmware
- Hardware



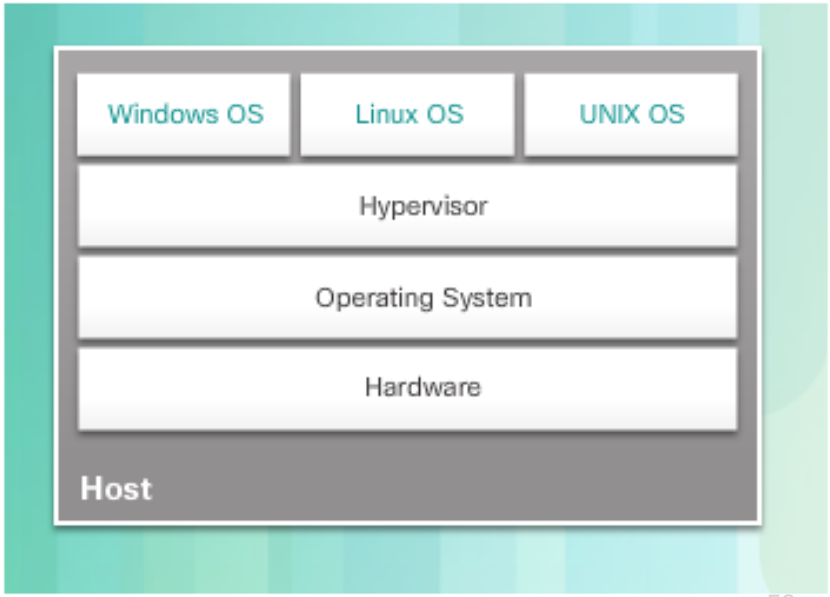
Las capas de abstracción

- En cada una de estas capas de abstracción, algún tipo de código de programación se utiliza como una interfaz entre la capa de abajo y la capa de arriba.
- Por ejemplo, el lenguaje de programación C se utiliza a menudo para programar el firmware que tiene acceso al hardware.
- Un hipervisor se instala entre el firmware y el sistema operativo. El hipervisor puede soportar múltiples instancias de sistemas operativos.



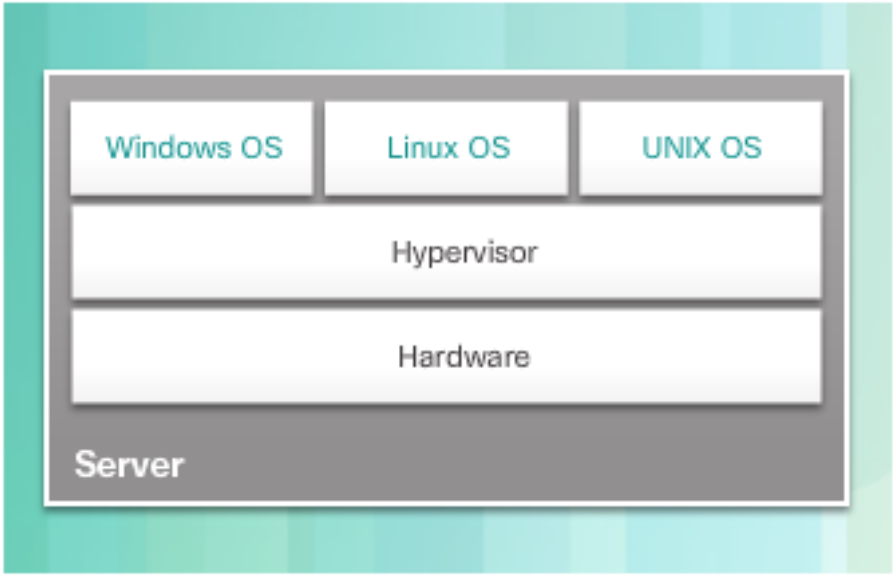
Los hipervisores de tipo 2

- Un hipervisor es un software que crea y ejecuta instancias de máquina virtual.
- Hipervisor de tipo 2 está instalado en el sistema operativo existentes, como Mac OS X, Windows o Linux.
- El equipo, en el que un hipervisor está apoyando una o más máquinas virtuales, es una máquina host.
- Los hipervisores Tipo 2; se llaman alojado hipervisores.
- Tipo común 2 hipervisores incluyen:
- Virtual PC
- VMware Estación de trabajo
- Oracle VM VirtualBox
- VMware Fusion
- Mac OS X Parallels

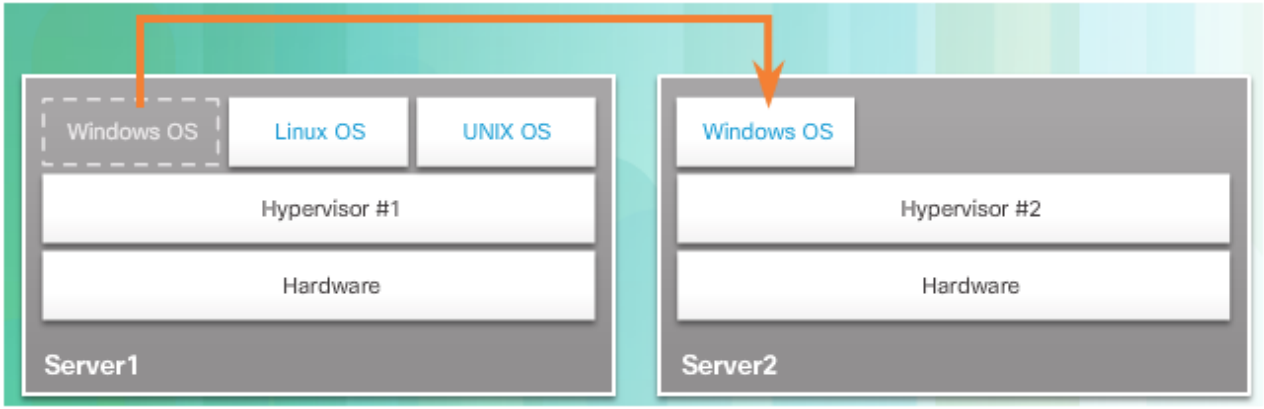


Los hipervisores de tipo 1

- Hipervisores de tipo 1 también se les llama "metal desnudo" porque el hipervisor se instala directamente en el servidor o hardware de red.
- Los hipervisores Tipo 1 tienen acceso directo a los recursos de hardware; por lo tanto, son más eficientes que las arquitecturas alojadas.
- Tipo 1 hipervisores populares incluyen:
- Citrix XenServer
- Microsoft Hyper-V 2008/2012
- Oracle VM Server para x86 / SPARC
- VMware ESXi



La instalación de una máquina virtual en un hipervisor



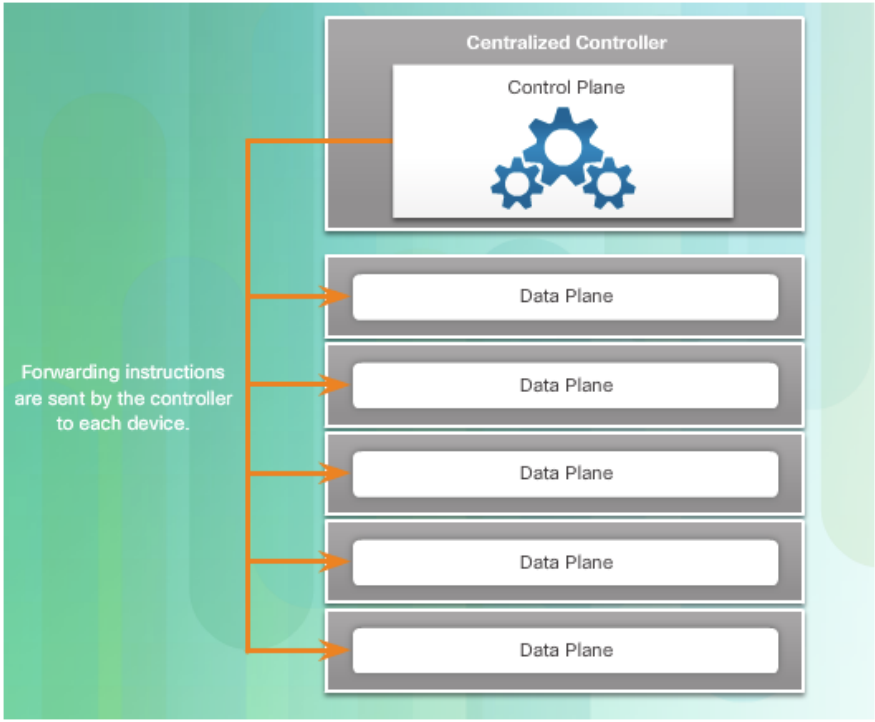
- Los hipervisores Tipo 1 requieren una "consola de administración" para gestionar el hipervisor.
- software de gestión se utiliza para gestionar múltiples servidores que utilizan el mismo hipervisor.
- La consola de administración puede consolidar de forma automática los servidores y encender o apagar los servidores según sea necesario. Por ejemplo, supongamos que se convierte en servidor 1 bajo de recursos. Para que haya más recursos disponibles, la consola de administración mueve la instancia de Windows para el hipervisor en el servidor 2.

La virtualización de red

- La virtualización de servidores oculta los recursos del servidor.
- Esto puede crear problemas si el centro de datos usa arquitecturas de red tradicionales.
- Por ejemplo, las (VLAN) utilizados por las MV deben ser asignados al mismo puerto del switch como el servidor físico que ejecuta el hipervisor.
- Los flujos de tráfico difieren sustancialmente del modelo cliente-servidor.
- Un centro de datos tiene una cantidad considerable de tráfico que se intercambian entre los servidores virtuales (en adelante, el tráfico Este-Oeste).
- Los flujos cambian de ubicación e intensidad con el tiempo, requiere un enfoque flexible.
- Las infraestructuras existentes pueden responder a las necesidades cambiantes relacionadas con la gestión de los flujos de tráfico mediante el uso de (QoS) y las configuraciones de nivel de seguridad para los flujos individuales.
- Sin embargo, en las grandes empresas que utilizan equipos de múltiples proveedores, cada vez que una nueva MV está activada, la reconfiguración necesaria puede ser muy lento.

Plano de control y Plano de datos

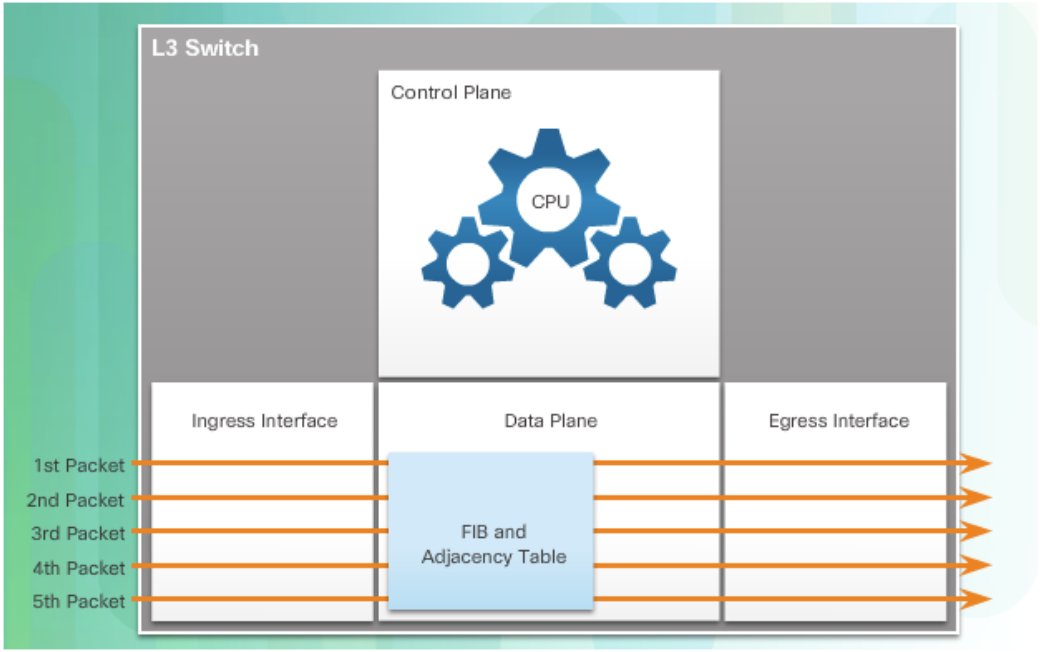
- Un dispositivo de red contiene los siguientes planos:
- **De control**: el cerebro del dispositivo.
- Se utiliza para tomar decisiones de envío.
- Contiene Capa 2 y Capa 3 mecanismos de desvío de ruta, tales como:
- Las tablas de enrutamiento de protocolo vecino y tablas de topología
- tablas de enrutamiento IPv4 e IPv6
- STP
- tabla ARP
- **De datos** (plano de reenvío), la matriz de conmutación que conecta los distintos puertos de red en un dispositivo.
- Se utiliza para reenviar los flujos de tráfico.



Cisco Express Forwarding (CEF) es una tecnología de conmutación de capa 3 avanzada, permite el envío de paquetes desde el plano de datos sin consultar el plano de control.

Plano de control y Plano de datos

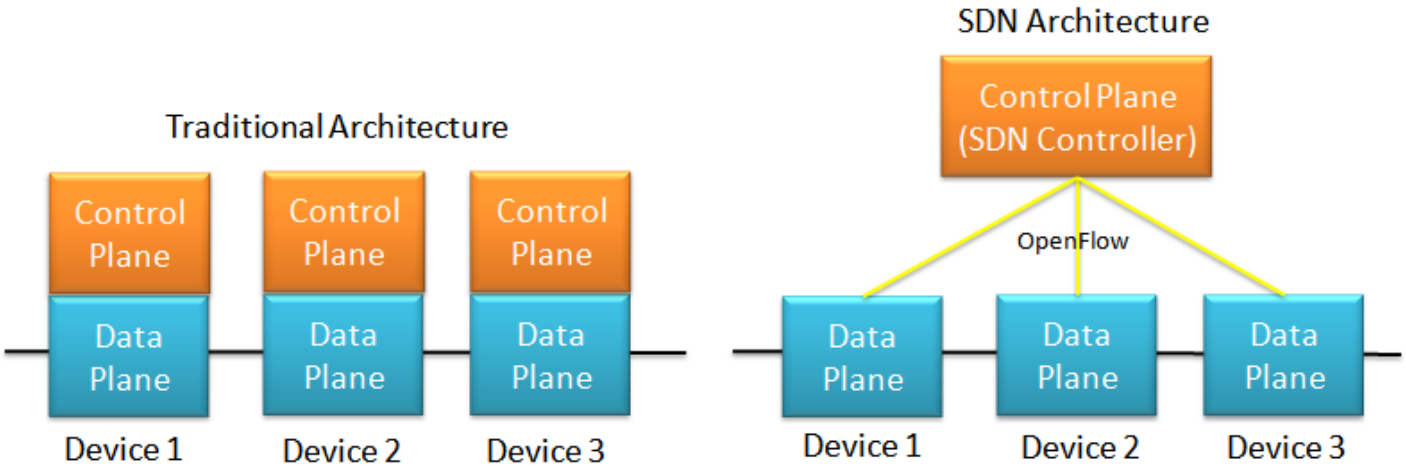
- CEF es una tecnología de conmutación avanzada capa 3 , IP que permite el reenvío de paquetes a ocurrir en el plano de datos sin consultar el plano de control.



La virtualización de red

- Dos arquitecturas de red para apoyar la virtualización de la red:
- **Redes definidas por software (SDN):** arquitectura de red virtualiza la red.
- **Infraestructura Cisco Aplicación Centric (ACI)** - Una solución de hardware diseñado para integrar la computación en nube y gestión de datos centralizado.
- Otras tecnologías incluidas como componentes en SDN y ACI:
- **OpenFlow**: gestiona el tráfico entre los router, switch, AP y un controlador.
- **OpenStack**: se utiliza a menudo con Cisco ACI.
- La Orquestación en la creación de redes es el proceso de automatizar el aprovisionamiento de componentes de red, tales como servidores, almacenamiento, switch, router y aplicaciones.
- Otros componentes incluyen la interfaz con el sistema de enrutamiento (I2RS), Interconexión transparente de un montón de enlaces (TRILL), Cisco FabricPath (FP), e IEEE 802.1aq ruta más corta puenteada (SPB).

Arquitectura SDN

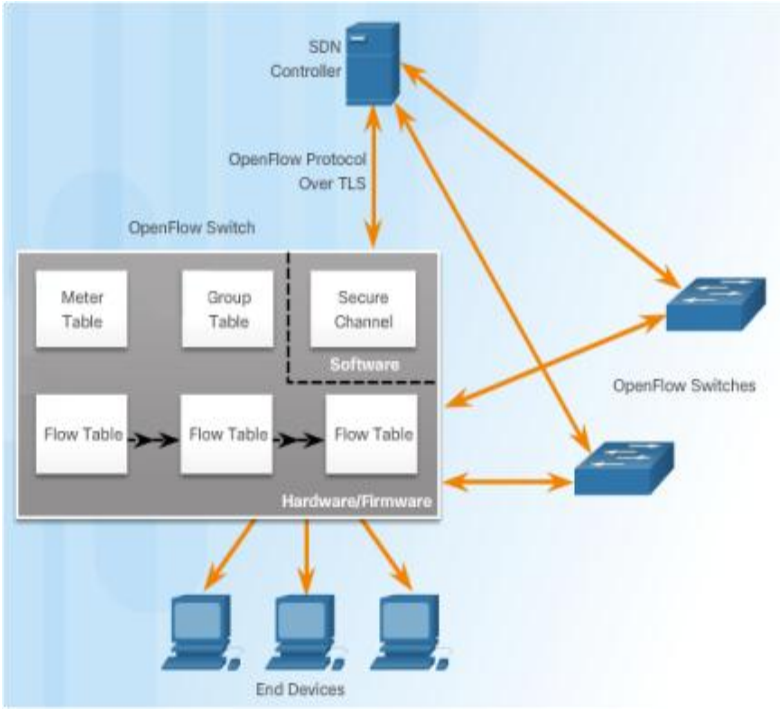


- El router tradicional o la arquitectura del switch, las funciones del plano de control y de datos se producen en el mismo dispositivo.

- Redes definidas por software (SDN) mueve el plano de control de cada dispositivo de red a una entidad central de inteligencia de red y la formulación de políticas denominado el controlador SDN.

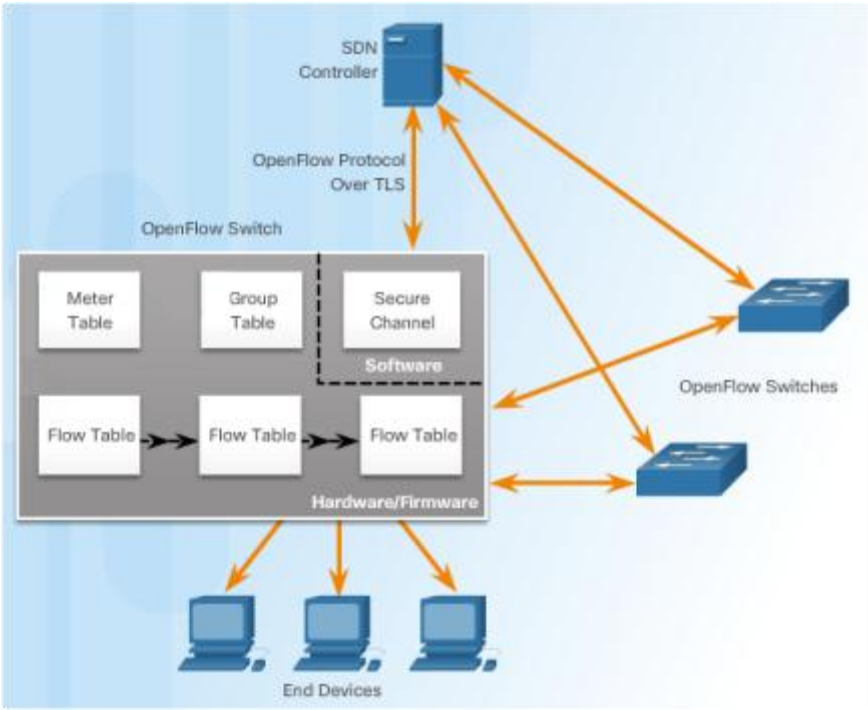
Controlador y Operaciones de SDN

- El controlador SDN define los flujos de datos producidos en el plano de datos SDN.
- Un flujo es una secuencia de paquetes que atraviesan una red que comparten un conjunto de valores.
- Todas las funciones complejas las realiza el controlador.
- El controlador llena las tablas de flujo para conmutar y gestionar las tablas de flujo.
- El controlador SDN se comunica con conmutadores compatibles con OpenFlow mediante protocolo OpenFlow.
- Este protocolo utiliza Transport Layer Security (TLS) para enviar las comunicaciones del plano de control sobre la red.
- Cada switch OpenFlow se conecta a otros switches OpenFlow.



Controlador y Operaciones de SDN

- Para el switch, un flujo es una secuencia de paquetes que coincide con una entrada específica en una tabla de flujo.
- Las tablas tienen los objetivos siguientes:
- Una tabla de flujo coincide con los paquetes de entrada a un flujo particular y especifica las funciones que se van a realizar en los paquetes.
- Un actualizador de la Tabla desencadena una serie de acciones relacionadas con el rendimiento en un flujo.
- Una tabla de flujo puede dirigir un flujo a un grupo, que puede accionar una variedad de acciones que afectan a uno o más flujos.



Controlador y Operaciones de SDN

- Cisco ha desarrollado la infraestructura de aplicaciones Centric (ACI) para ayudar a las organizaciones que no tienen el deseo o la habilidad para programar el uso de herramientas de SDN, para automatizar la red.

- Cisco ACI es una solución de hardware especialmente diseñado para integrar la computación en nube y gestión de datos central.

- En un nivel alto, el elemento de la política de la red se elimina del plano de datos.

- Esto simplifica la forma en que las redes de centros de datos se crean.

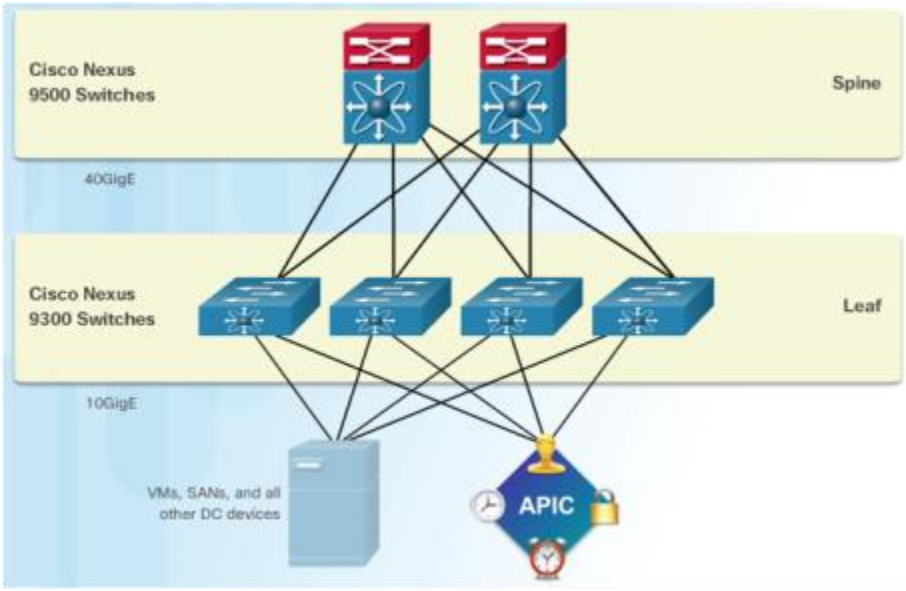
Topologia espina-borde (Spine-Leaf)

- Cisco ACI de fabrica está compuesto por el APIC y los switch de la serie Cisco Nexus 9000 utilizando dos niveles (spine-leaf) en la topología de borde.

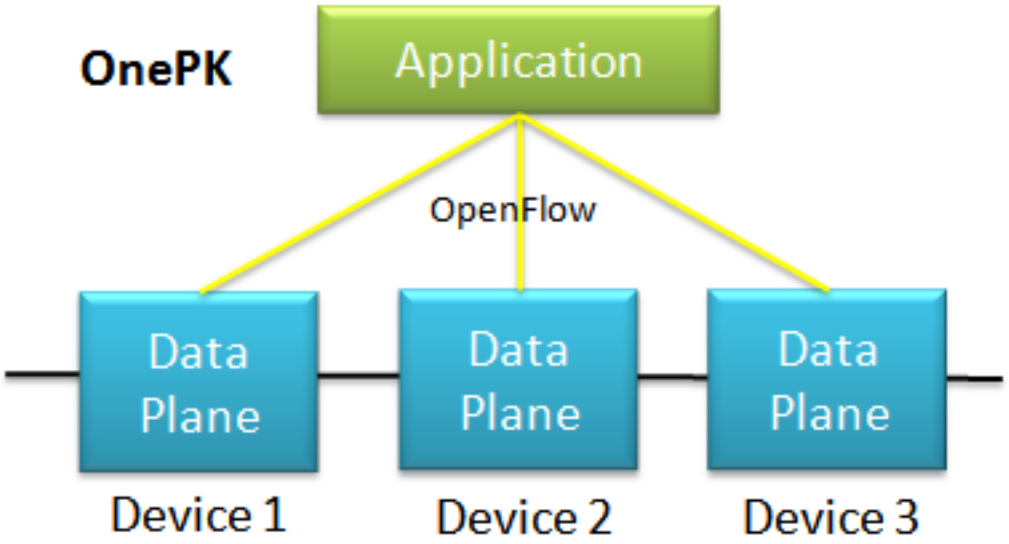
- Los switch de los bordes siempre se adhieren a otros bordes, pero nunca se adhieren uno al otro.

- Del mismo modo, en la columna vertebral solamente los switch de adjuntan al borde y al núcleo de los otros switches (no mostrado).

- En esta topología de dos niveles, todo esta a un salto de todos lo demás.



Tipos SDN

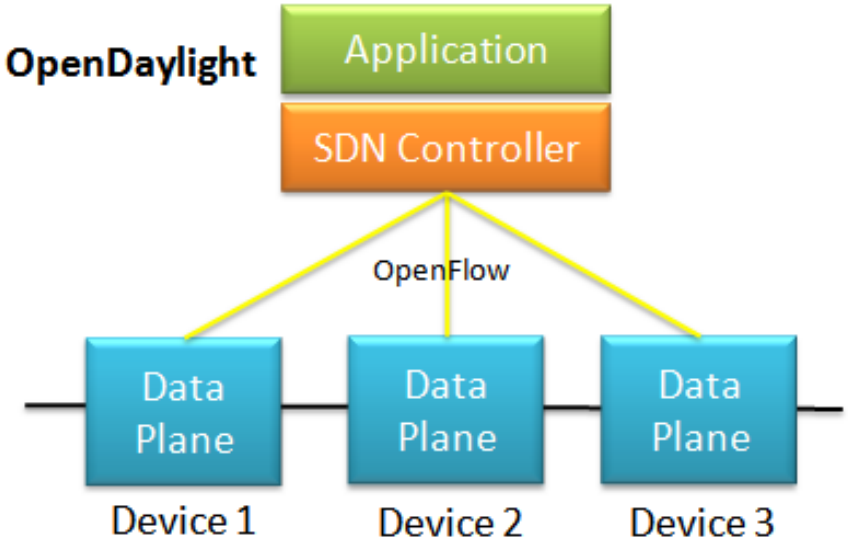


- **Dispositivo basado en SDN** - son programables por aplicaciones que se ejecutan en el propio dispositivo o en un servidor en la red.

- Cisco OnePK es un ejemplo de un SDN basado en dispositivo.

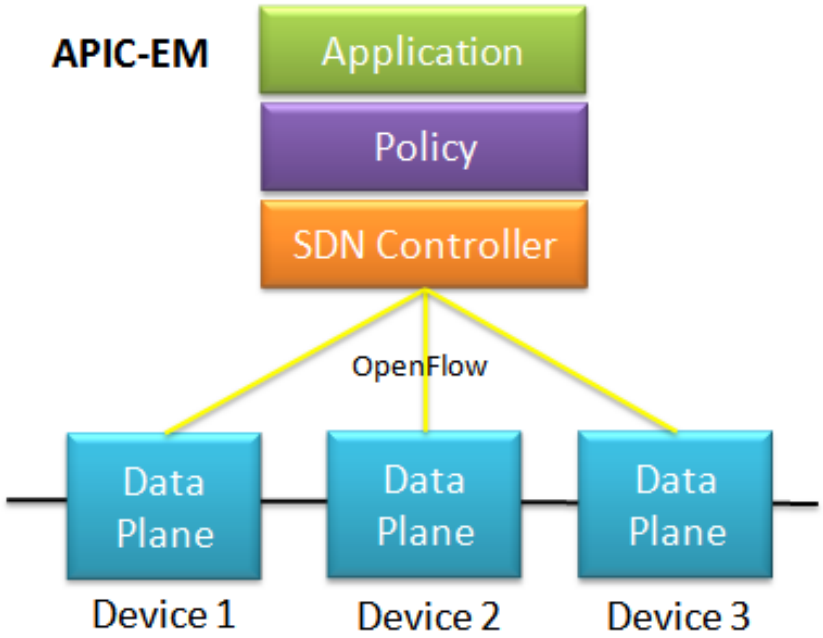
- Se permite a los programadores crear aplicaciones utilizando C, Java y Python, integrar e interactuar con los dispositivos de Cisco.

Tipos SDN



- **SDN basada en controlador:** Utiliza un controlador centralizado que tiene conocimiento de todos los dispositivos en la red.
- Las aplicaciones pueden interactuar con el controlador responsable de la gestión de dispositivos y la manipulación de los flujos de tráfico en toda la red.
- El controlador SDN abierto Cisco es una distribución comercial de OpenDaylight.

Tipos SDN



- **SDN basado en políticas:** Similar al controlador SDN basado en un controlador centralizado tiene una vista de todos los dispositivos en la red.
- SDN basado en políticas incluye una capa adicional que la política funciona a un nivel más alto de abstracción.
- Utiliza aplicaciones integradas que automatizan las tareas de configuración avanzada a través de un flujo de trabajo guiado y de interfaz gráfica de usuario fácil de usar sin conocimientos de programación necesarios.
- Cisco APIC-EM es un ejemplo de este tipo de SDN.

Caracteristicas de APIC-EM

SDN basado en políticas es la más robusta, que prevée un mecanismo simple para controlar y gestionar las políticas en toda la red.

Cisco APIC-EM ofrece las siguientes características:

Descubrimiento

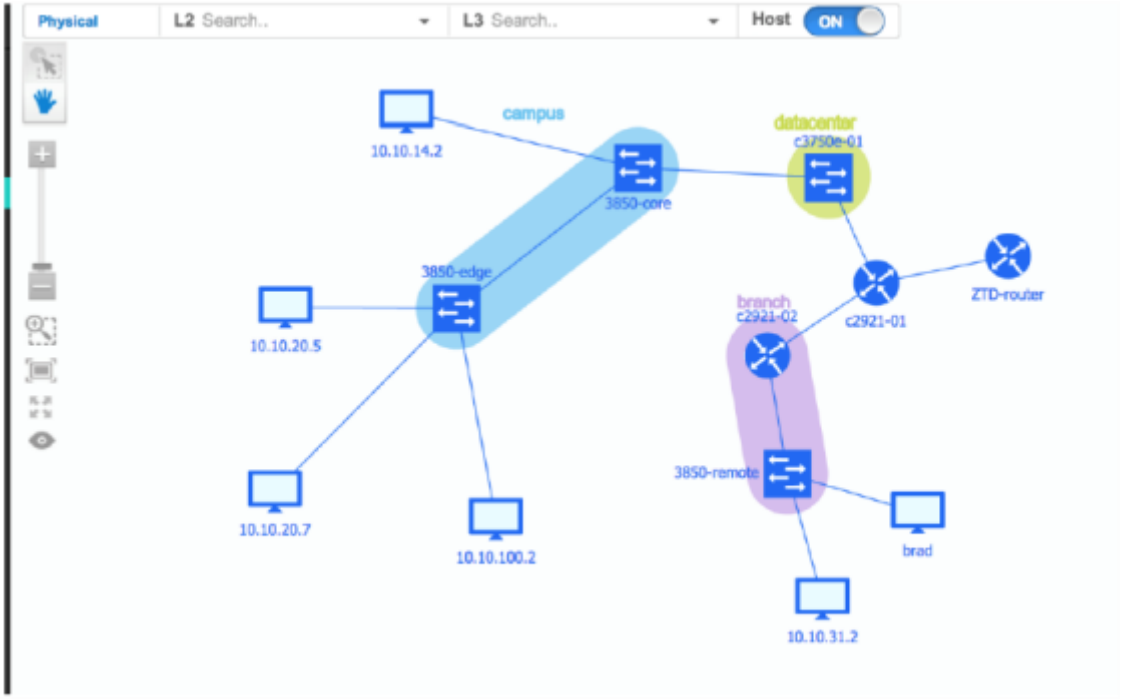
Inventario de dispositivos

Inventario de acogida

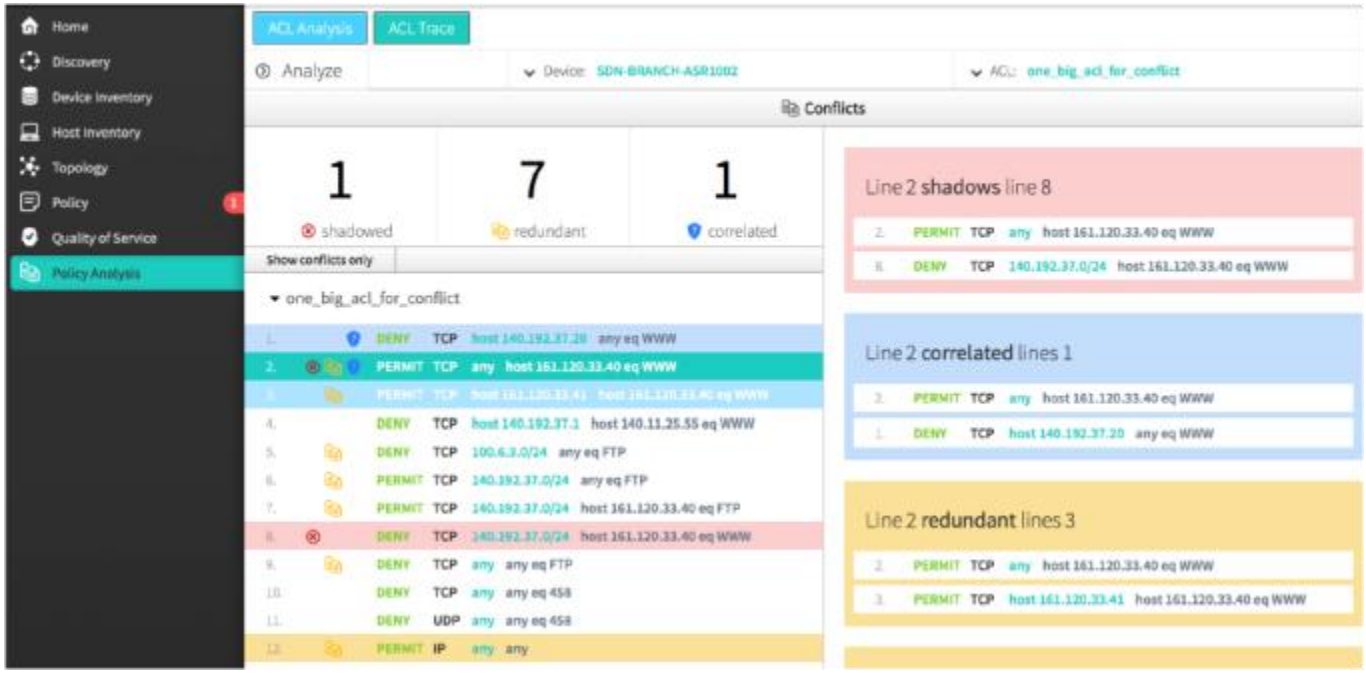
topología

Política

Análisis de políticas



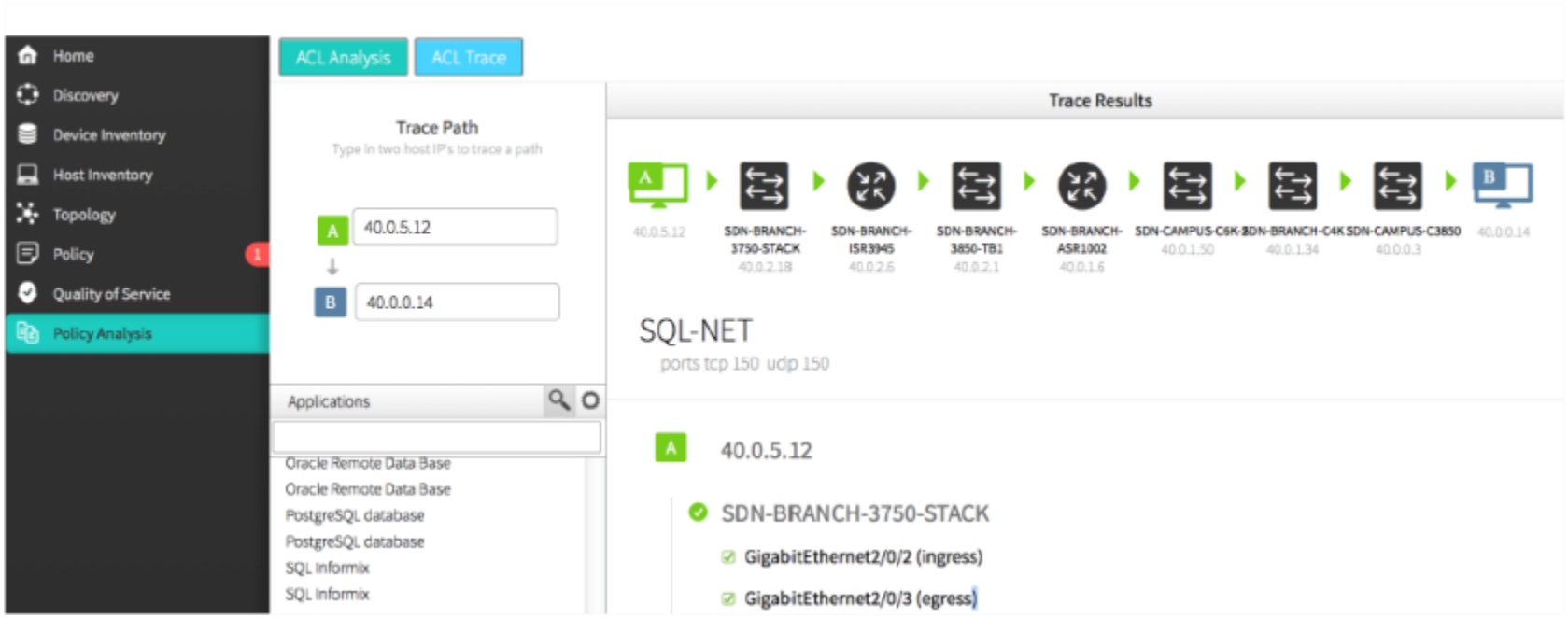
Analisis de ACL APIC-EM



- Examina las ACL en los dispositivos, la búsqueda de redundancias, contradictorias, o entradas ocultas.

- Análisis ACL permite la inspección y el interrogatorio a través de toda la red, dejando al descubierto los problemas y conflictos.

Analisis de ACL APIC-EM



- Examina ACL específicas sobre el camino entre dos nodos finales, mostrando los posibles problemas.

IP SLA

- Los Acuerdos de Nivel de Servicio IP (SLAs) son una característica del Cisco IOS que permite el análisis de los niveles de servicio IP.

- SLA IP utilizan el tráfico para medir el rendimiento de red entre dos dispositivos de red, múltiples ubicaciones de red, o en varias rutas de red generado.

- La supervisión del rendimiento se puede hacer en cualquier momento y en cualquier lugar, sin tener que desplegar una conexión física.
- ping
- traceroute

Configuracion de IP SLA

- Operación de IP ICMP SLA eco proporciona las siguientes mediciones:
- Supervisión de la disponibilidad (estadísticas de pérdida de paquetes)
- La supervisión del rendimiento (latencia y tiempo de respuesta)
- Funcionamiento de la red (de extremo a extremo conectividad)
- SHOW IP SLA verifica la aplicación si la operación de IP SLA deseado está disponible en el dispositivo fuente.
- Opción IP SLA eco ICMP aparece como disponible

```
Router# show ip sla application
      IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
      icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
      dns, udpJitter, dhcp, ftp, VoIP, icmpJitter
      802.1agEcho VLAN, Port, 802.1agJitter VLAN, Port, y1731Delay
      y1731Loss, udpApp, wspApp, mcast, generic

Supported Features:
      IPSLAs Event Publisher

IP SLAs low memory water mark: 61167610
Estimated system max number of entries: 44800

Estimated number of configurable operations: 44641
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0
Time of last change in whole IP SLAs: *20:27:15.935 UTC Wed Jan 27 2016
```

Configuración de IP SLA

- ICMP Echo configuracion y pasos de ICMP echo

Step	Command	Purpose
1	**configure terminal**	Enter global configuration mode.
2	**ip sla** *operation-number*	Create an IP SLA operation and enter IP SLA configuration mode. The operation number is a unique number used to identify the operation being configured.
3	**icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-id*]	Configure the IP SLA operation as an ICMP Echo operation and enter ICMP echo configuration mode. • *destination-ip-address* | *destination-hostname*-Specify the destination IP address or hostname. • (Optional) **source-ip** {*ip-address* | *hostname*}-Specify the source IP address or hostname. When a source IP address or hostname is not specified, the IP SLA chooses the IP address nearest to the destination. • (Optional) **source-interface** *interface-id*-Specify the source interface for the operation.
4	**frequency** *seconds*	(Optional) Set the rate at which a specified IP SLA operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds.
5	**exit**	Exit ICMP echo configuration mode, and return to global configuration mode.

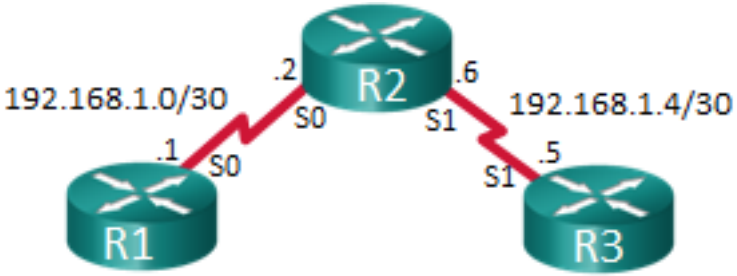
Configuración de IP SLA

- ICMP Echo configuracion y pasos de ICMP echo

6	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**]	Configure the scheduling parameters for an individual IP SLAs operation. • *operation-number* Enter the RTR entry number. • (Optional) **life**-Set the operation to run indefinitely (**forever**) or for a specific number of *seconds*. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour) • (Optional) **start-time**-Enter the time for the operation to begin collecting information: – To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month. If no month is entered, the default is the current month. – Enter **pending** to select no information collection until a start time is selected. – Enter **now** to start the operation immediately. – Enter **after** *hh:mm:ss* to indicate that the operation should start after the entered time has elapsed. • (Optional) **ageout** *seconds*-Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds; the default is 0 seconds (never ages out). • (Optional) **recurring**-Set the operation to automatically run every day.

Configuración de IP SLA

- Ejemplo de configuracion




```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip sla 1
R1(config-ip-sla)# icmp-echo 192.168.1.5
R1(config-ip-sla-echo)# frequency 30
R1(config-ip-sla-echo)# exit
R1(config)#ip sla schedule 1 start-time now life forever
R1(config)# end
R1#
```

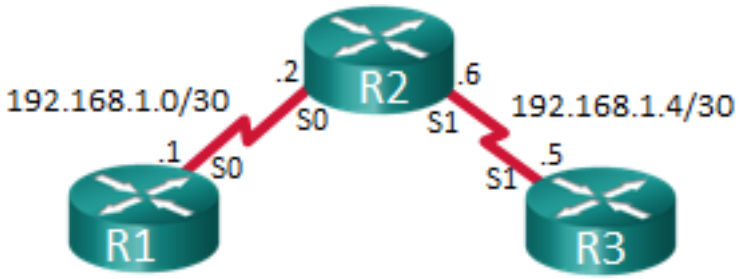
Configuración de IP SLA

- Verificando la configuracion

```
R1# show ip sla configuration
IP SLAs Infrastructure Engine-III
Entry number: 1
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: icmp-echo
Target address/Source address: 192.168.1.5/0.0.0.0
Type Of Service parameter: 0x0
Request size (ARR data portion): 28
Verify data: No
Vrf Name:
Schedule:
   Operation frequency (seconds): 30  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 1
   Statistic distribution interval (milliseconds): 20
Enhanced History:
History Statistics:
   Number of history Lives kept: 0
   Number of history Buckets kept: 15
   History Filter Type: None
```

Configuración de IP SLA

- Desplegar estadisticas




```
R1# show ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 1
      Latest RTT: 12 milliseconds
Latest operation start time: 00:12:31 UTC Thu Nov 26 2015
Latest operation return code: OK
Number of successes: 57
Number of failures: 0
Operation time to live: Forever
```

- El último ping a la interfaz S1 de R3 tiene un tiempo de ida y vuelta de 12 milisegundos.
- Desde que se inició la operación, se ha puesto a prueba la conectividad de 57 veces sin fallas.