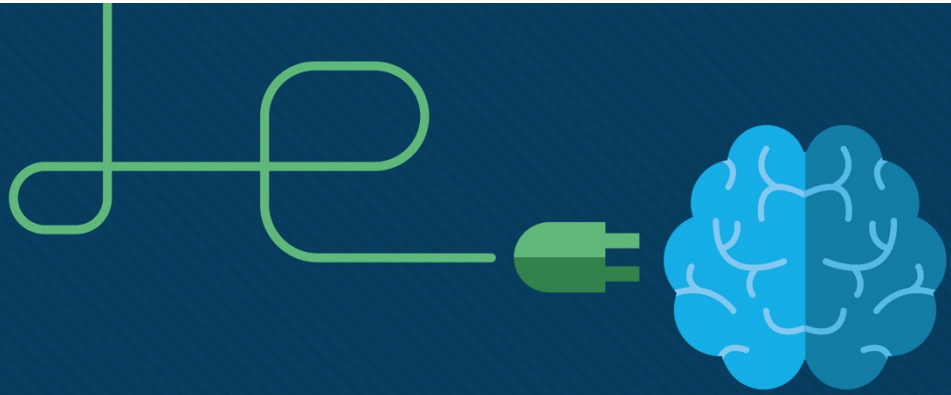


Lecture#10: Transport Layer

Operation and Services : Communication Process

Introduction to Networks v7.0 (ITN) Module: 14

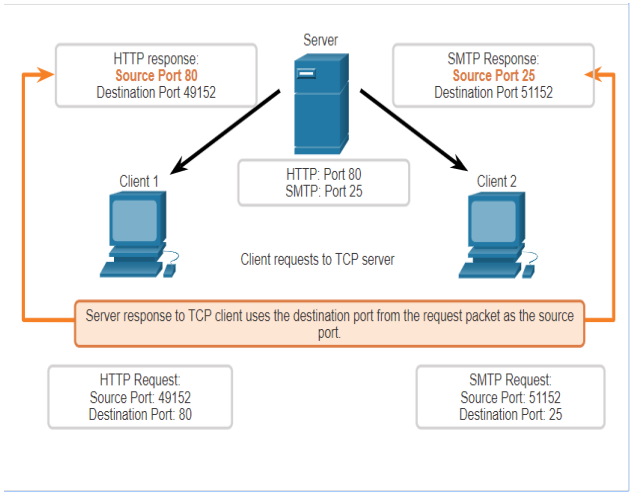
10.1.1 TCP Communication

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TCP Server Processes

Each application process running on a server is configured to use a port number.

- An individual server cannot have two services assigned to the same port number within the same transport layer services.
- An active server application assigned to a specific port is considered open, which means that the transport layer accepts, and processes segments addressed to that port.
- Any incoming client request addressed to the correct socket is accepted, and the data is passed to the server application.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

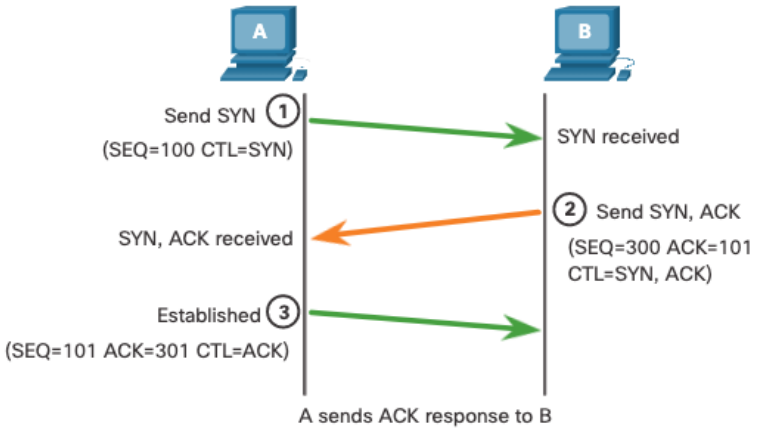
TCP Communication Process

TCP Connection Establishment

Step 1: The initiating client requests a client-to-server communication session with the server.

Step 2: The server acknowledges the client-to-server communication session and requests a server-to-client communication session.

Step 3: The initiating client acknowledges the server-to-client communication session.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

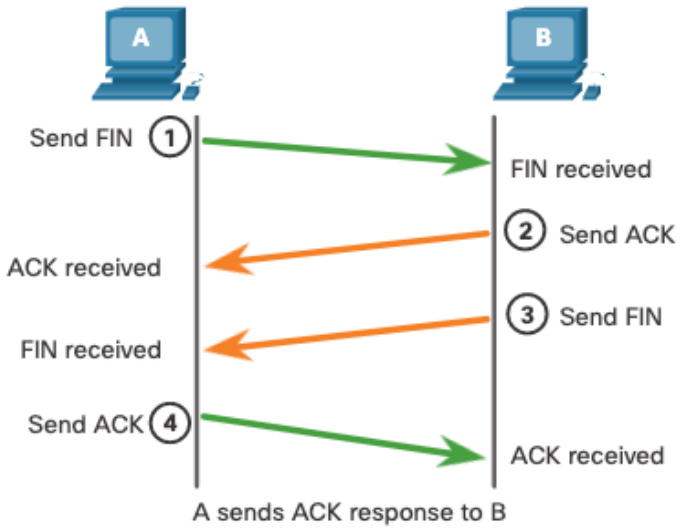
TCP Connection Termination

Step 1: When the client has no more data to send in the stream, it sends a segment with the FIN flag set.

Step 2: The server sends an ACK to acknowledge the receipt of the FIN to terminate the session from client to server.

Step 3: The server sends a FIN to the client to terminate the server-to-client session.

Step 4: The client responds with an ACK to acknowledge the FIN from the server.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TCP Three-Way Handshake Analysis

Functions of the **Three-Way Handshake**:

- It establishes that the destination device is present on the network.
- It verifies that the destination device has an active service and is accepting requests on the destination port number that the initiating client intends to use.
- It informs the destination device that the source client intends to establish a communication session on that port number.

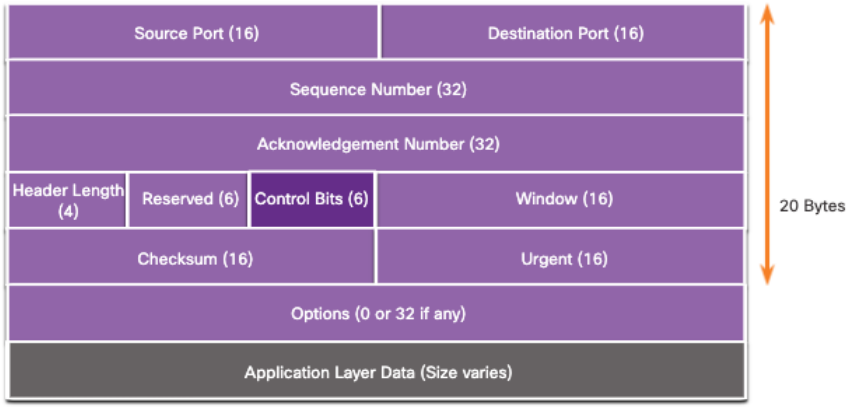
After the communication is completed the sessions are closed, and the connection is terminated. The connection and session mechanisms enable TCP reliability function.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TCP Three-Way Handshake Analysis (Cont.)

The six control bit flags are as follows:

- **URG** - Urgent pointer field significant
- **ACK** - Acknowledgment flag used in connection establishment and session termination
- **PSH** - Push function
- **RST** - Reset the connection when an error or timeout occurs
- **SYN** - Synchronize sequence numbers used in connection establishment
- **FIN** - No more data from sender and used in session termination



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TCP Communication Process

Video TCP 3-Way Handshake

The video covers the following:

- TCP 3-Way Handshake
- Termination of a TCP conversation

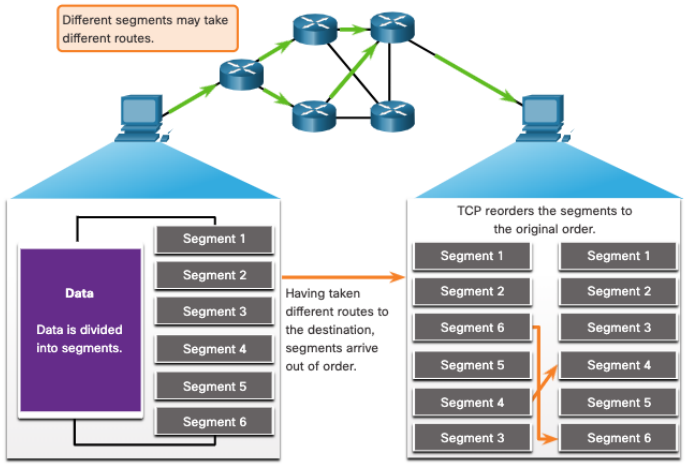
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

10.1.2 Reliability and Flow Control

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TCP Reliability- Guaranteed and Ordered Delivery

- TCP can also help maintain the flow of packets so that devices do not become overloaded.
- There may be times when TCP segments do not arrive at their destination or arrive out of order.
- All the data must be received and the data in these segments must be reassembled into the original order.
- Sequence numbers are assigned in the header of each packet to achieve this goal.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video -TCP Reliability- Sequence Numbers and Acknowledgments

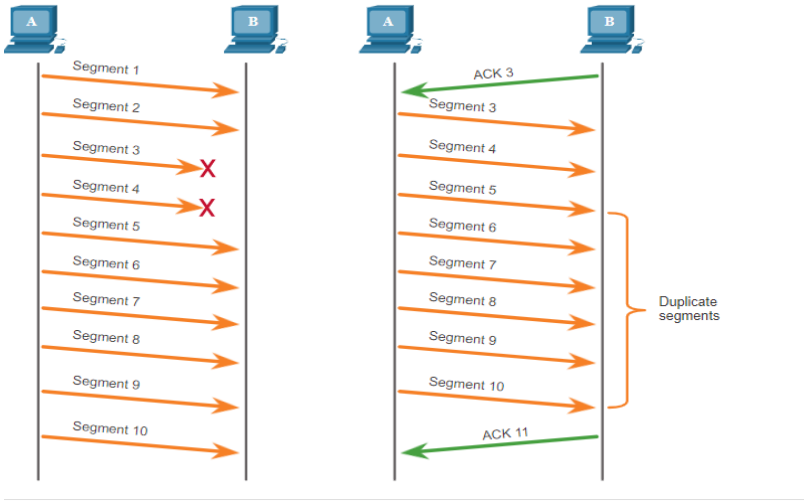
This video depicts a simplified example of the TCP operations.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TCP Reliability – Data Loss and Retransmission

No matter how well designed a network is, data loss occasionally occurs.

TCP provides methods of managing these segment losses. Among these is a mechanism to retransmit segments for unacknowledged data.

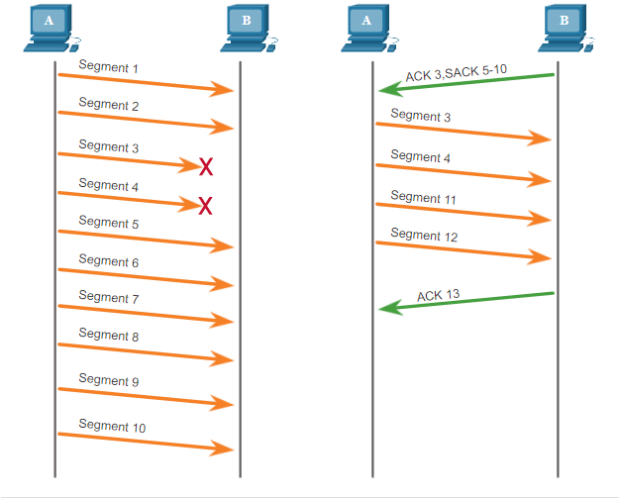


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TCP Reliability – Data Loss and Retransmission (Cont.)

Host operating systems today typically employ an optional TCP feature called selective acknowledgment (SACK), negotiated during the three-way handshake.

If both hosts support SACK, the receiver can explicitly acknowledge which segments (bytes) were received including any discontinuous segments.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video - TCP Reliability – Data Loss and Retransmission

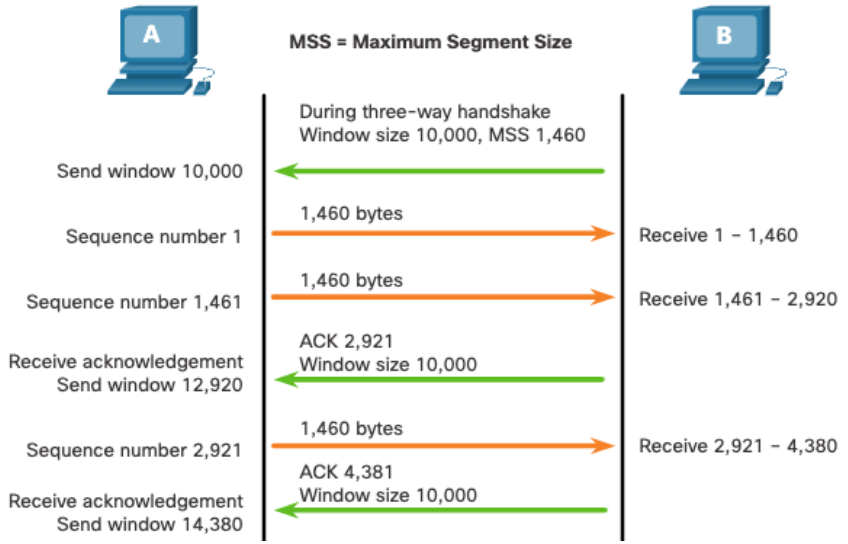
This video shows the process of resending segments that are not initially received by the destination.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TCP Flow Control – Window Size and Acknowledgments

TCP also provides mechanisms for flow control as follows:

- Flow control is the amount of data that the destination can receive and process reliably.
- Flow control helps maintain the reliability of TCP transmission by adjusting the rate of data flow between source and destination for a given session.

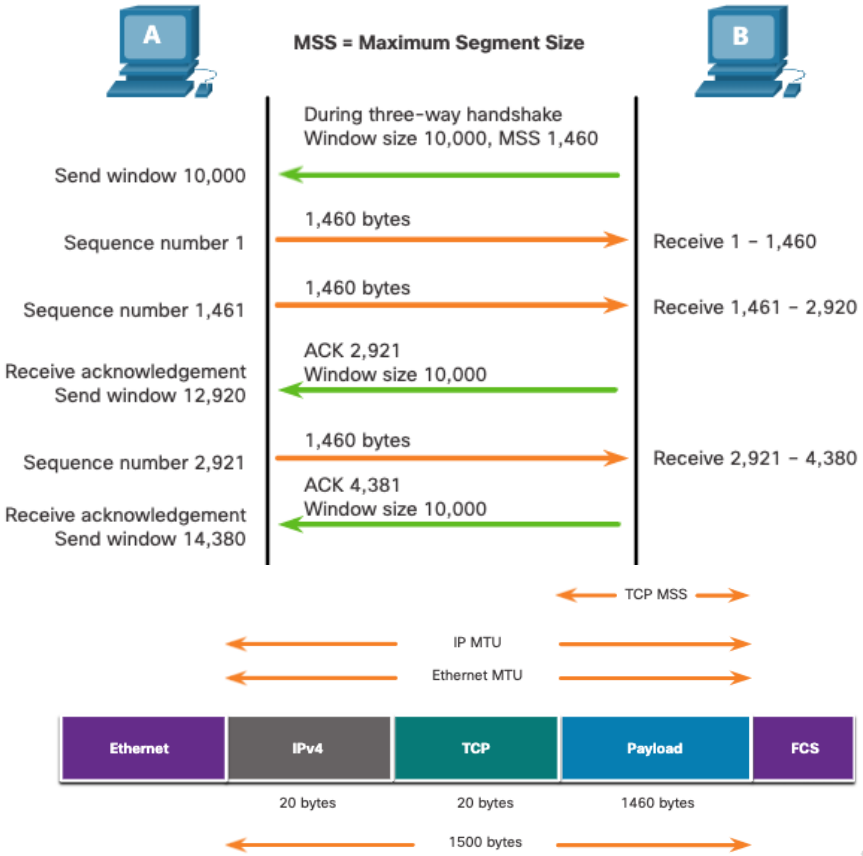


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TCP Flow Control – Maximum Segment Size

Maximum Segment Size (MSS) is the maximum amount of data that the destination device can receive.

- A common MSS is 1,460 bytes when using IPv4.
- A host determines the value of its MSS field by subtracting the IP and TCP headers from the Ethernet maximum transmission unit (MTU), which is 1500 bytes be default.
- 1500 minus 60 (20 bytes for the IPv4 header and 20 bytes for the TCP header) leaves 1460 bytes.

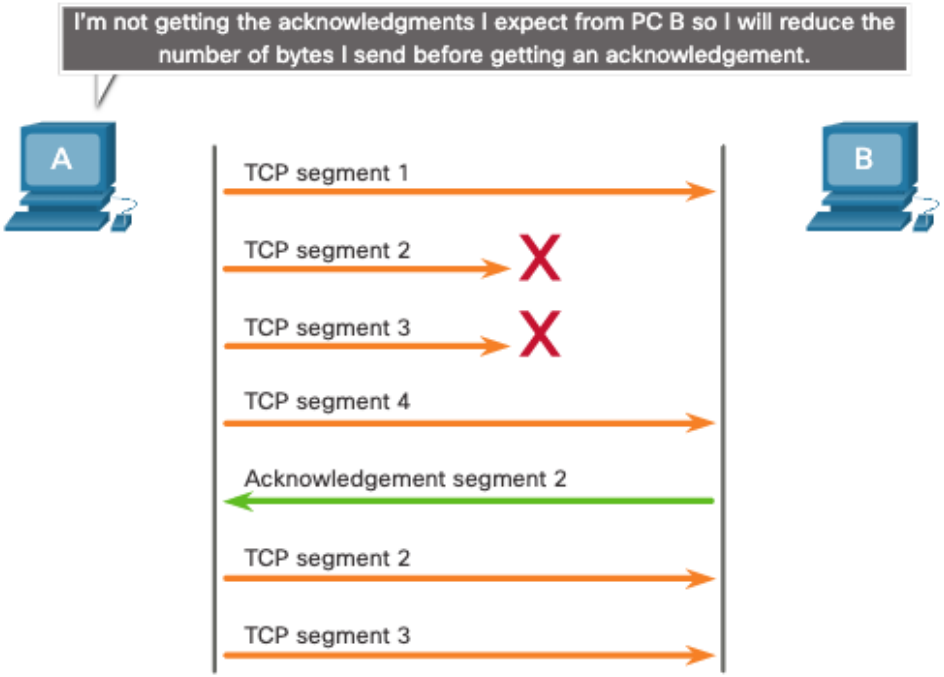


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TCP Flow Control – Congestion Avoidance

When congestion occurs on a network, it results in packets being discarded by the overloaded router.

To avoid and control congestion, TCP employs several congestion handling mechanisms, timers, and algorithms.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

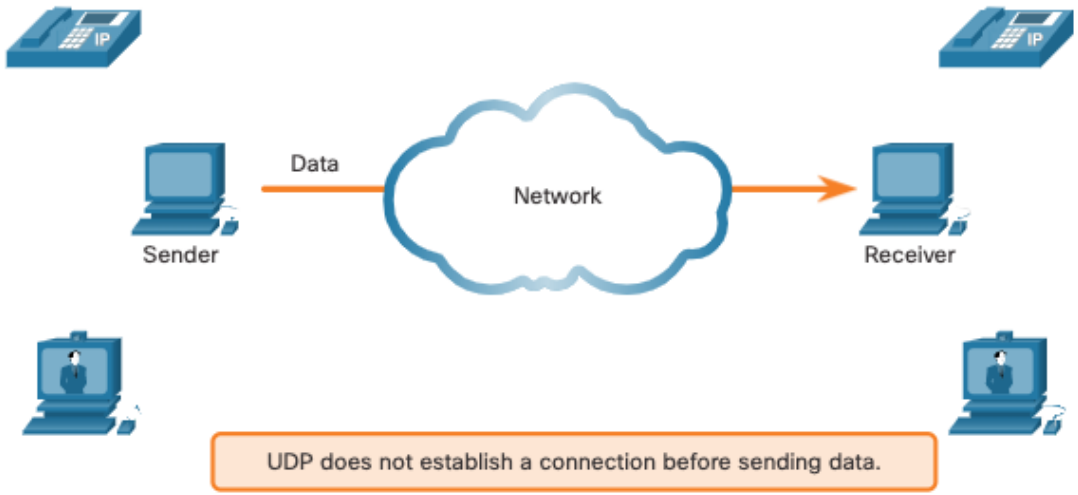
10.2.1 UDP Communication

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

UDP Communication

UDP Low Overhead versus Reliability

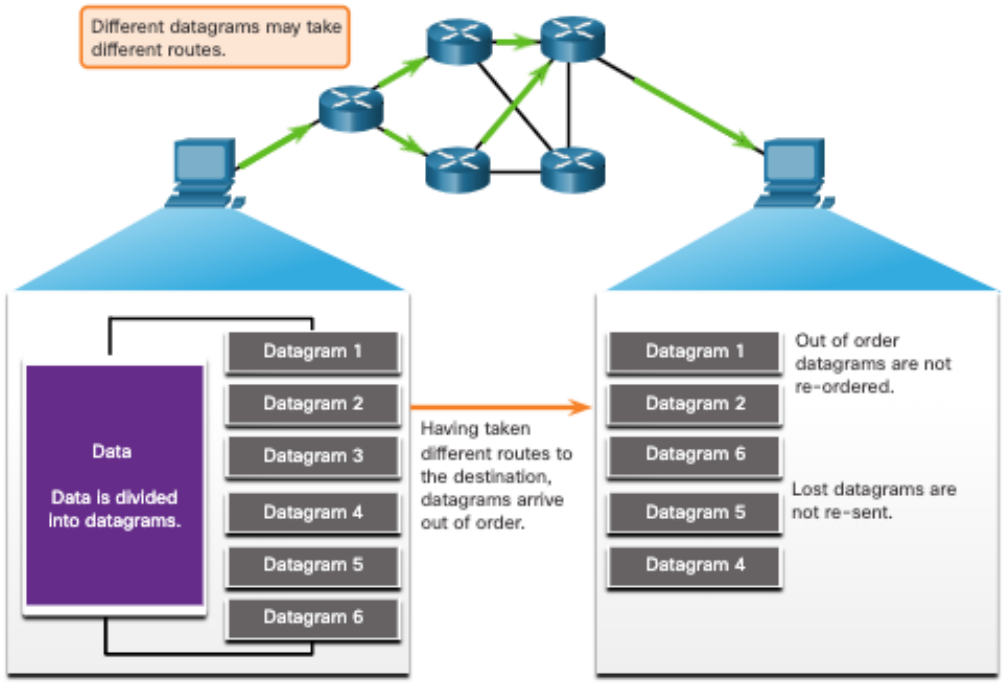
UDP does not establish a connection. UDP provides low overhead data transport because it has a small datagram header and no network management traffic.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

UDP Datagram Reassembly

- UDP does not track sequence numbers the way TCP does.
- UDP has no way to reorder the datagrams into their transmission order.
- UDP simply reassembles the data in the order that it was received and forwards it to the application.



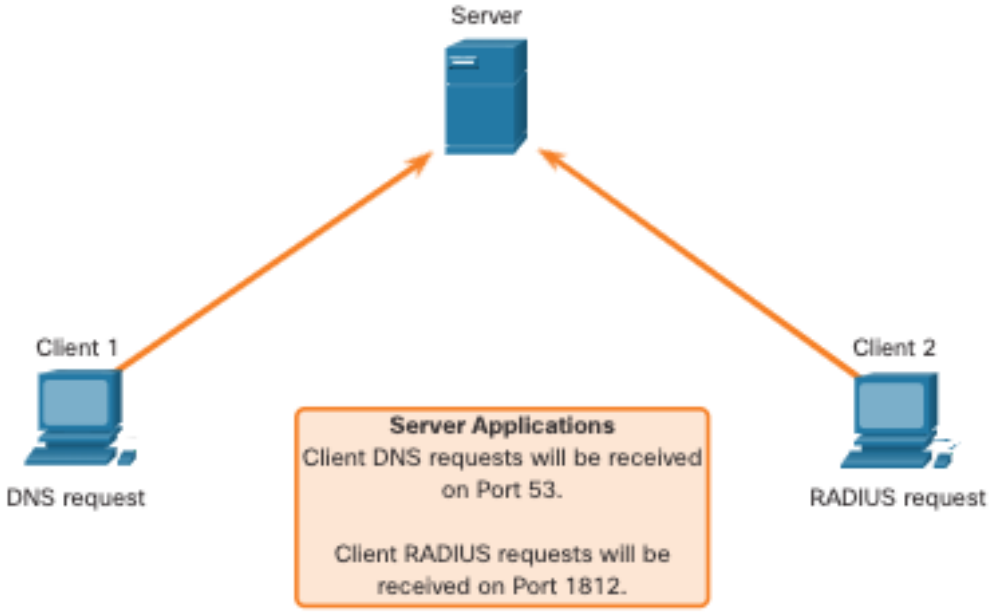
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

UDP Communication

UDP Server Processes and Requests

UDP-based server applications are assigned well-known or registered port numbers.

UDP receives a datagram destined for one of these ports, it forwards the application data to the appropriate application based on its port number.

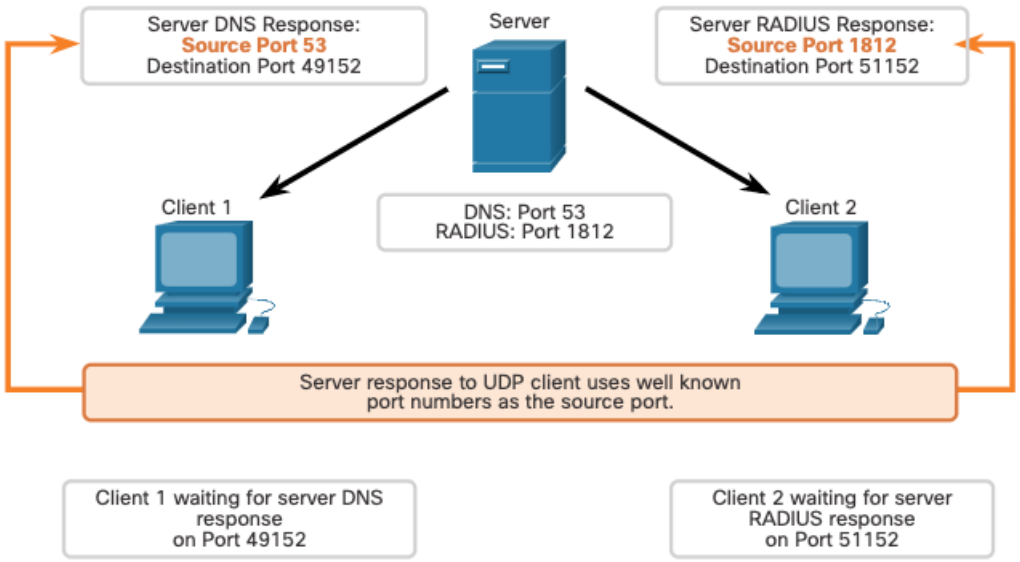


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

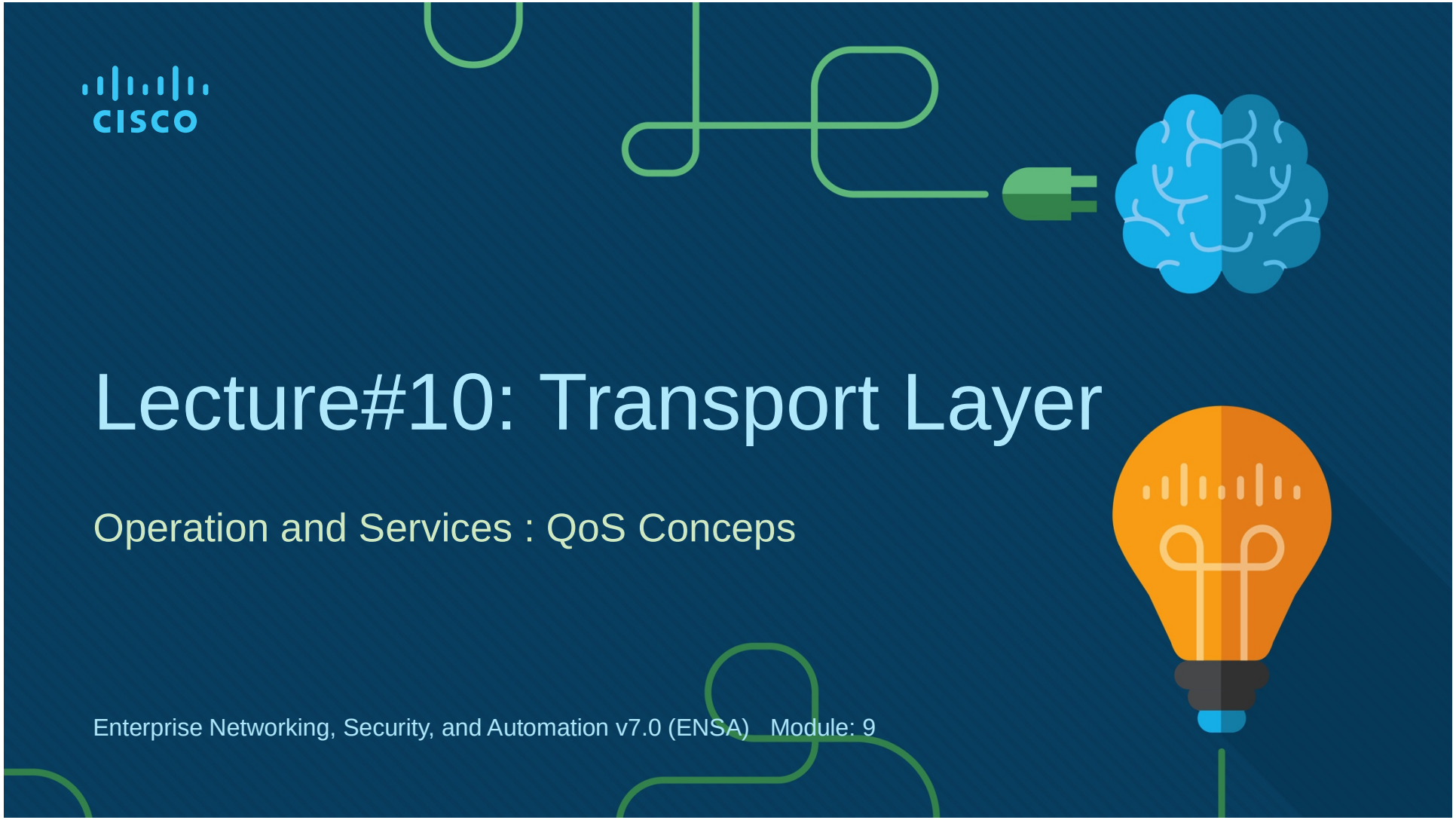
UDP Communication

UDP Client Processes

- The UDP client process dynamically selects a port number from the range of port numbers and uses this as the source port for the conversation.
- The destination port is usually the well-known or registered port number assigned to the server process.
- After a client has selected the source and destination ports, the same pair of ports are used in the header of all datagrams in the transaction.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


Lecture#10: Transport Layer
Operation and Services : QoS Conceps
Enterprise Networking, Security, and Automation v7.0 (ENSA) Module: 9

10.3.1 Network Transmission Quality

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network Transmission Quality

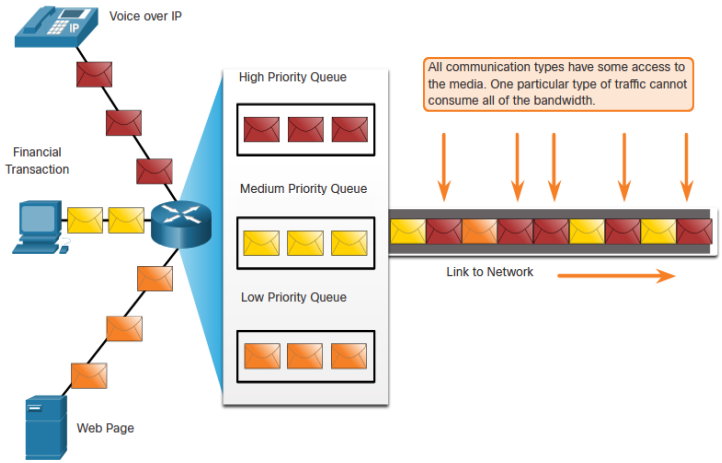
Video – The Purpose of QoS

This video explains Quality of Service (QoS) and why it is needed.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Prioritizing Traffic

- When traffic volume is greater than what can be transported across the network, devices queue (hold) the packets in memory until resources become available to transmit them.
- Queuing packets causes delay because new packets cannot be transmitted until previous packets have been processed.
- If the number of packets to be queued continues to increase, the memory within the device fills up and packets are dropped.
- One QoS technique that can help with this problem is to classify data into multiple queues, as shown in the figure.



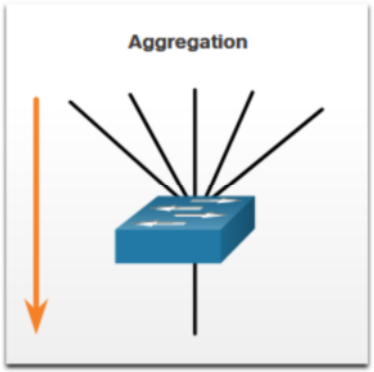
Note: A device implements QoS only when it is experiencing some type of congestion.

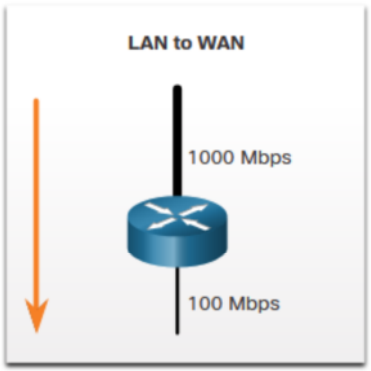
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

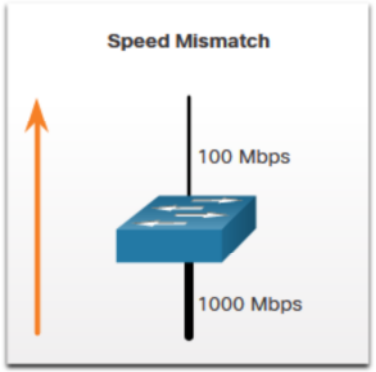
Network Transmission Quality

Bandwidth, Congestion, Delay, and Jitter

- Network **bandwidth** is measured in the number of bits that can be transmitted in a single second, or bits per second.
- Network **congestion** causes **delay**. An interface experiences congestion when it is presented with more traffic than it can handle. Network congestion points are ideal candidates for QoS mechanisms.
- The typical congestion points are **aggregation**, **speed mismatch**, and **LAN to WAN**.







© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Bandwidth, Congestion, Delay, and Jitter (Cont.)

Delay or **latency** refers to the time it takes for a packet to travel from the source to the destination.

- Fixed delay is the amount of time a specific process takes, such as how long it takes to place a bit on the transmission media.
- Variable delay takes an unspecified amount of time and is affected by factors such as how much traffic is being processed.
- Jitter is the variation of delay of received packets.

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

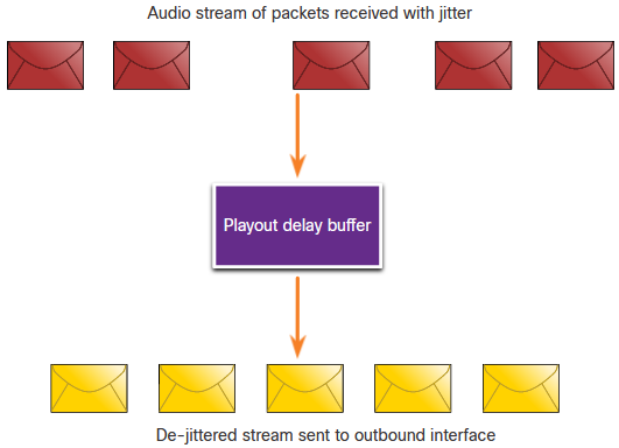
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network Transmission Quality

Packet Loss

Without QoS mechanisms, time-sensitive packets, such as real-time video and voice, are dropped with the same frequency as data that is not time-sensitive.

- When a router receives a Real-Time Protocol (RTP) digital audio stream for Voice over IP (VoIP), it compensates for the jitter that is encountered using a playout delay buffer.
- The playout delay buffer buffers these packets and then plays them out in a steady stream.



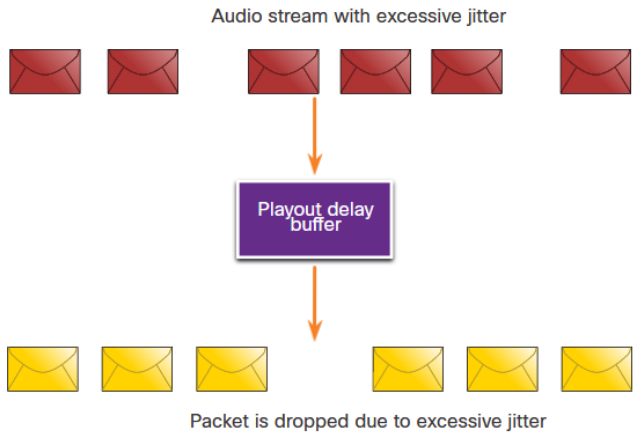
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network Transmission Quality

Packet Loss (Cont.)

If the jitter is so large that it causes packets to be received out of the range of the play out buffer, the out-of-range packets are discarded and dropouts are heard in the audio.

- For losses as small as one packet, the digital signal processor (DSP) interpolates what it thinks the audio should be and no problem is audible to the user.
- When jitter exceeds what the DSP can do to make up for the missing packets, audio problems are heard.



***Note**: In a properly designed network, packet loss should be near zero*

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

10.3.2 Traffic Characteristics

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Traffic Characteristics

Video – Traffic Characteristics

This video will explain the characteristics of voice, video, and data traffic.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Traffic Characteristics

Network Traffic Trends

In the **early 2000s**, the predominant types of IP traffic were voice and data.

- Voice traffic has a predictable bandwidth need and known packet arrival times.
- Data traffic is not real-time and has unpredictable bandwidth need.
- Data traffic can temporarily burst, as when a large file is being downloaded. This bursting can consume the entire bandwidth of a link.

More **recently**, video traffic has become the increasingly important to business communications and operations.

- According to the Cisco Visual Networking Index (VNI), video traffic represented 70% of all traffic in 2017.
- By 2022, video will represent 82% of all traffic.
- Mobile video traffic will reach 60.9 exabytes per month by 2022.

The **type of demands** that voice, video, and data traffic place on the network are very different.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Traffic Characteristics

Voice

Voice traffic is predictable and smooth and very sensitive to delays and dropped packets.

- Voice packets must receive a higher priority than other types of traffic.
- Cisco products use the RTP port range 16384 to 32767 to prioritize voice traffic.

Voice can **tolerate** a certain amount of latency, jitter, and loss without any noticeable effects

Latency should be no more than 150 milliseconds (ms).

- Jitter should be no more than 30 ms, and packet loss no more than 1%.
- Voice traffic requires at least 30 Kbps of bandwidth.

Voice Traffic Characteristics	One-Way Requirements
• Smooth • Benign • Drop sensitive • Delay sensitive • UPD priority	• Latency ≤ 150ms • Jitter ≤ 30ms • Loss ≤ 1% Bandwidth (30-128 Kbps)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Traffic Characteristics

Video

Video traffic tends to be unpredictable, inconsistent, and bursty. Compared to voice, video is less resilient to loss and has a higher volume of data per packet.

- The number and size of video packets varies every 33 ms based on the content of the video.
- UDP ports such as 554, are used for the Real-Time Streaming Protocol (RSTP) and should be given priority over other, less delay-sensitive, network traffic.
- **Latency** should be no more than 400 milliseconds (ms). Jitter should be no more than 50 ms, and video packet loss should be no more than 1%. Video traffic requires at least 384 Kbps of bandwidth.

Video Traffic Characteristics	One-Way Requirements
• Bursty • Greedy • Drop sensitive • Delay sensitive • UPD priority	• Latency ≤ 200-400 ms • Jitter ≤ 30-50 ms • Loss ≤ 0.1 – 1% • Bandwidth (384 Kbps - 20 Mbps)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Traffic Characteristics

Data

Data applications that have no tolerance for data loss, such as email and web pages, use TCP to ensure that if packets are lost in transit, they will be resent.

- Data traffic can be smooth or bursty.
- Network control traffic is usually smooth and predictable.

Some TCP applications can consume a large portion of network capacity. FTP will consume as much bandwidth as it can get when you download a large file, such as a movie or game.

Data Traffic Characteristics

- Smooth/bursty
- Benign/greedy
- Drop insensitive
- Delay insensitive
- TCP Retransmits

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Traffic Characteristics

Data (Cont.)

Data traffic is relatively insensitive to drops and delays compared to voice and video. Quality of Experience or QoE is important to consider with data traffic.

- Does the data come from an interactive application?
- Is the data mission critical?

Factor	Mission Critical	Not Mission Critical
Interactive	Prioritize for the lowest delay of all data traffic and strive for a 1 to 2 second 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.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

10.3.3 Queuing Algorithms

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Queuing Algorithms

Video – QoS Algorithms

This video will cover the following:

- FIFO Queuing (absence of QoS)
- Weighted Fair Queuing (WFQ)
- Class Based Weighted Fair Queuing (CBWFQ)
- Low Latency Queuing (LLQ)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Queuing Algorithms

Queuing Overview

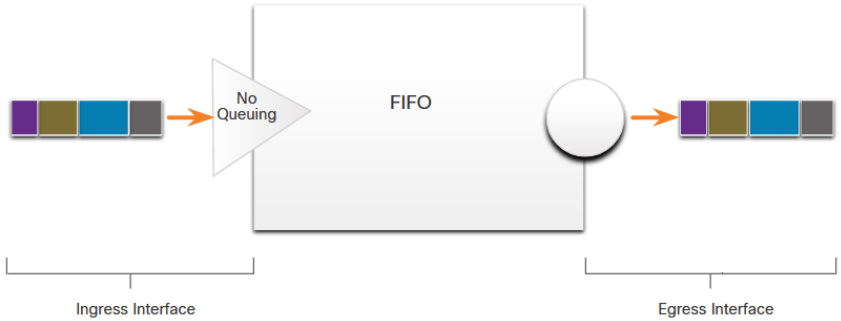
- The **QoS policy** implemented by the network administrator becomes active when congestion occurs on the link.
- **Queuing** is a congestion management tool that can buffer, prioritize, and, if required, reorder packets before being transmitted to the destination.
- A number of **queuing algorithms** are available:
  - First-In, First-Out (FIFO)
  - Weighted Fair Queuing (WFQ)
  - Class-Based Weighted Fair Queuing (CBWFQ)
  - Low Latency Queuing (LLQ)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Queuing Algorithms

First in First Out

- First In First Out (FIFO) queuing buffers and forwards packets in the order of their arrival.
- FIFO has no concept of priority or classes of traffic and consequently, makes no decision about packet priority.
  - There is only one queue, and all packets are treated equally.
  - Packets are sent out an interface in the order in which they arrive.



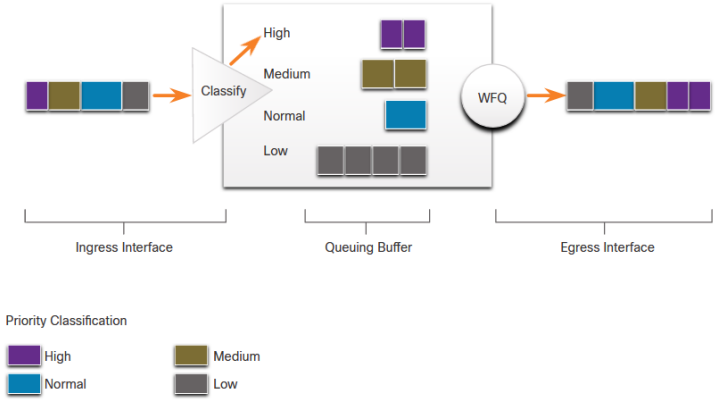
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Queuing Algorithms

Weighted Fair Queuing (WFQ)

Weighted Fair Queuing (WFQ) is an automated scheduling method that provides fair bandwidth allocation to all network traffic.

- WFQ applies priority, or weights, to identified traffic, classifies it into conversations or flows, and then determines how much bandwidth each flow is allowed relative to other flows.
- WFQ classifies traffic into different flows based on source and destination IP addresses, MAC addresses, port numbers, protocol, and Type of Service (ToS) value.
- WFQ is not supported with tunneling and encryption because these features modify the packet content information required by WFQ for classification..



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Queuing Algorithms

Class-Based Weighted Fair Queuing (CBWFQ)

Class-Based Weighted Fair Queuing (CBWFQ) extends the standard WFQ functionality to provide support for user-defined traffic classes.

- Traffic classes are defined based on match criteria including protocols, access control lists (ACLs), and input interfaces.
- Packets satisfying the match criteria for a class constitute the traffic for that class.
- A FIFO queue is reserved for each class, and traffic belonging to a class is directed to the queue for that class.
- A class can be assigned characteristics, such as bandwidth, weight, and maximum packet limit. The bandwidth assigned to a class is the guaranteed bandwidth delivered during congestion.
- Packets belonging to a class are subject to the bandwidth and queue limits, which is the maximum number of packets allowed to accumulate in the queue, that characterize the class.

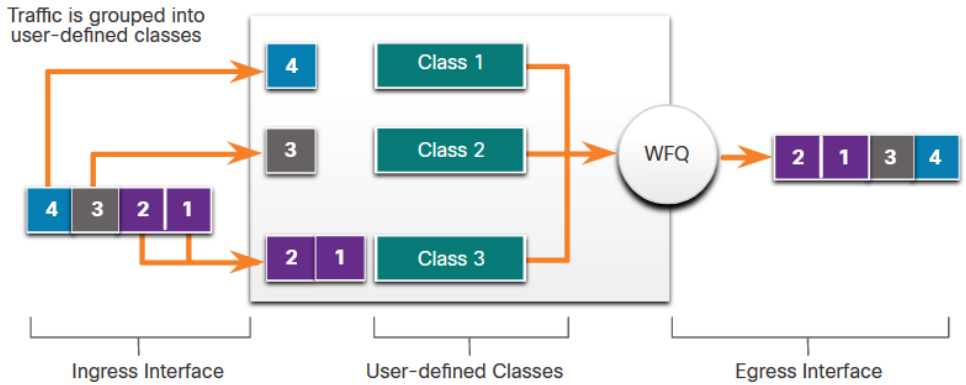
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Class-Based Weighted Fair Queuing (CBWFQ) (Cont.)

After a queue has reached its configured queue limit, adding more packets to the class causes tail drop or packet drop to take effect, depending on how class policy is configured.

- Tail drop discards any packet that arrives at the tail end of a queue that has completely used up its packet-holding resources.

- This is the default queuing response to congestion. Tail drop treats all traffic equally and does not differentiate between classes of service.



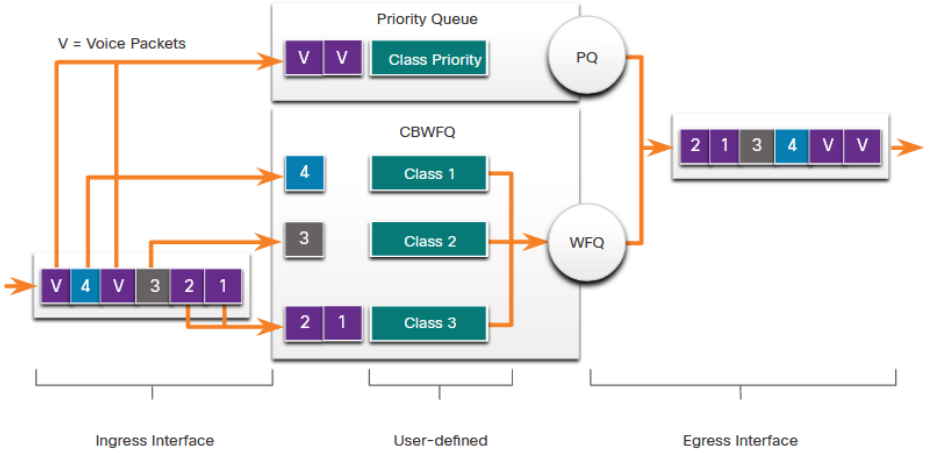
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Queuing Algorithms

Low Latency Queuing (LLQ)

The Low Latency Queuing (LLQ) feature brings strict priority queuing (PQ) to CBWFQ.

- Strict PQ allows delay-sensitive packets such as voice to be sent before packets in other queues.
- LLQ allows delay-sensitive packets such as voice to be sent first (before packets in other queues), giving delay-sensitive packets preferential treatment over other traffic.
- Cisco recommends that only voice traffic be directed to the priority queue.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

10.3.4 QoS Models

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

QoS Models

Video – QoS Models

This video will cover the following:

- Best-effort model
- Integrated services (IntServ)
- Differentiated services (DiffServ)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

QoS Models

Selecting an Appropriate QoS Policy Model

There are three models for implementing QoS. QoS is implemented in a network using either IntServ or DiffServ.

- IntServ provides the highest guarantee of QoS, it is very resource-intensive, and therefore, not easily scalable.
- DiffServ is less resource-intensive and more scalable.
- IntServ and DiffServ are sometimes co-deployed in network QoS implementations.

Model	Description
Best-effort model	• Not 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. • 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. • 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.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

QoS Models

Best Effort

The basic design of the internet is best-effort packet delivery and provides no guarantees.

- The best-effort model treats all network packets in the same way, so an emergency voice message is treated the same way that a digital photograph attached to an email is treated.
- Benefits and drawbacks of the best effort model:

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

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

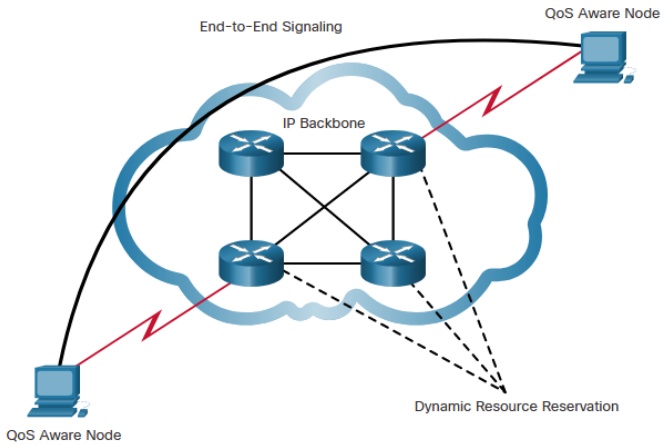
QoS Models

Integrated Services

IntServ delivers the end-to-end QoS that real-time applications require.

- Explicitly manages network resources to provide QoS to individual flows or streams, sometimes called microflows.
- Uses resource reservation and admission-control mechanisms as building blocks to establish and maintain QoS.

- Uses a connection-oriented approach. Each individual communication must explicitly specify its traffic descriptor and requested resources to the network.
- The edge router performs admission control to ensure that available resources are sufficient in the network.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

QoS Models

Integrated Services (Cont.)

In the IntServ model, the application requests a specific kind of service from the network before sending data.

- The application informs the network of its traffic profile and requests a particular kind of service that can encompass its bandwidth and delay requirements.
- IntServ uses the Resource Reservation Protocol (RSVP) to signal the QoS needs of an application's traffic along devices in the end-to-end path through the network.
- If network devices along the path can reserve the necessary bandwidth, the originating application can begin transmitting. If the requested reservation fails along the path, the originating application does not send any data.

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

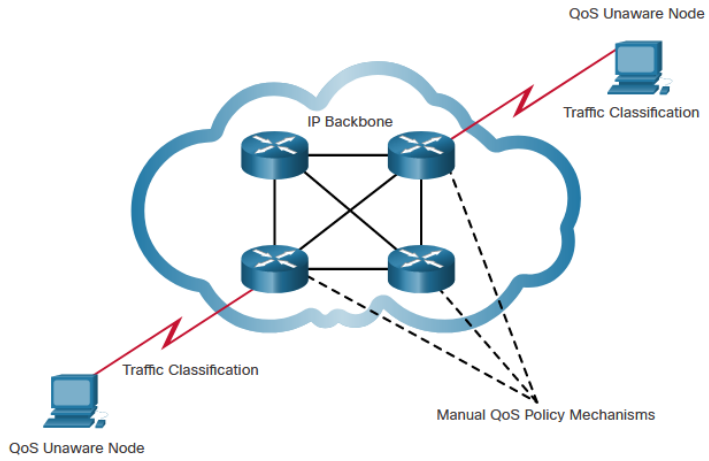
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

QoS Models

Differentiated Services

The differentiated services (DiffServ) QoS model specifies a simple and scalable mechanism for classifying and managing network traffic.

- Is not an end-to-end QoS strategy because it cannot enforce end-to-end guarantees.
- Hosts forward traffic to a router which classifies the flows into aggregates (classes) and provides the appropriate QoS policy for the classes.
- Enforces and applies QoS mechanisms on a hop-by-hop basis, uniformly applying global meaning to each traffic class to provide both flexibility and scalability.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

QoS Models

Differentiated Services (Cont.)

- DiffServ divides network traffic into classes based on business requirements. Each of the classes can then be assigned a different level of service.
- As the packets traverse a network, each of the network devices identifies the packet class and services the packet according to that class.
- It is possible to choose many levels of service with DiffServ.

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

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


CISCO