Network Topologies and Communication

Computer Networks

Author: Eng. Carlos Andrés Sierra, M.Sc.
carlos.andres.sierra.v@gmail.com

Lecturer
Computer Engineer
School of Engineering
Universidad Distrital Francisco José de Caldas

2024-I

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Outline

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Outline

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Network Topologies

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Bus Topology

Pros:

- The **bus topology** is easy to install and requires less cable than other topologies.
- It is easy to add new devices to the network.
- It is easy to troubleshoot and repair the network.
- It is easy to expand the network by adding new devices.

Cons:

- The **bus topology** is not very scalable and can become slow as the number of devices on the network increases.
- If the main cable fails, the entire network will fail.
- The bus topology is not very secure, as all devices on the network can see all data transmitted on the network.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Bus Topology

Pros:

- The **bus topology** is easy to install and requires less cable than other topologies.
- It is easy to add new devices to the network.
- It is easy to troubleshoot and repair the network.
- It is easy to expand the network by adding new devices.

Cons:

- The **bus topology** is not very scalable and can become slow as the number of devices on the network increases.
- If the main cable fails, the entire network will fail.
- The bus topology is not very secure, as all devices on the network can see all data transmitted on the network.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Ring Topology

Pros:

- The **ring topology** is easy to install and requires less cable than other topologies.
- It is easy to add new devices to the network.
- All devices on the network have equal access to the network.
- The ring topology is fault-tolerant, as data can be transmitted in both directions around the ring.

Cons:

- The **ring topology** is not very scalable and can become slow as the number of devices on the network increases.
- It is difficult to troubleshoot and repair the network.
- Security is a concern, as all devices on the network can see all data transmitted on the network.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Ring Topology

Pros:

- The **ring topology** is easy to install and requires less cable than other topologies.
- It is easy to add new devices to the network.
- All devices on the network have equal access to the network.
- The ring topology is fault-tolerant, as data can be transmitted in both directions around the ring.

Cons:

- The **ring topology** is not very scalable and can become slow as the number of devices on the network increases.
- It is difficult to troubleshoot and repair the network.
- Security is a concern, as all devices on the network can see all data transmitted on the network.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Star Topology

Pros:

- The **star topology** uses a central hub or switch to connect all devices on the network.
- It is easy to expand the network by adding new devices to the central hub or switch.
- It is easy to troubleshoot and repair the network, as each device is connected to the central hub or switch.
- The star topology is fault-tolerant, as data can still be transmitted between devices even if one device fails.

Cons:

- The **star topology** is more expensive than other topologies, as it requires more cable and more devices.
- If the central hub or switch fails, the entire network will fail.
- The star topology is not very scalable, as the central hub or switch can become a bottleneck as the number of devices on the network increases.

Star Topology

Pros:

- The **star topology** uses a central hub or switch to connect all devices on the network.
- It is easy to expand the network by adding new devices to the central hub or switch.
- It is easy to troubleshoot and repair the network, as each device is connected to the central hub or switch.
- The star topology is fault-tolerant, as data can still be transmitted between devices even if one device fails.

Cons:

- The **star topology** is more expensive than other topologies, as it requires more cable and more devices.
- If the central hub or switch fails, the entire network will fail.
- The star topology is not very scalable, as the central hub or switch can become a bottleneck as the number of devices on the network increases.

Tree Topology

Pros:

- The **tree topology** is a combination of the bus and star topologies.
- It is easy to expand the network by adding new devices to the parent hub or switch.
- It is easy to troubleshoot and repair the network, as each device is connected to the parent hub or switch.
- The tree topology is fault-tolerant, as data can still be transmitted between devices even if one device fails.

Cons:

- The **tree topology** is more expensive than other topologies, as it requires more cable and more devices.
- If the parent hub or switch fails, the entire sub-network will fail.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Tree Topology

Pros:

- The **tree topology** is a combination of the bus and star topologies.
- It is easy to expand the network by adding new devices to the parent hub or switch.
- It is easy to troubleshoot and repair the network, as each device is connected to the parent hub or switch.
- The tree topology is fault-tolerant, as data can still be transmitted between devices even if one device fails.

Cons:

- The **tree topology** is more expensive than other topologies, as it requires more cable and more devices.
- If the parent hub or switch fails, the entire sub-network will fail.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Mesh Topology

Pros:

- The **mesh topology** is the most reliable and fault-tolerant topology.
- It is easy to expand the network by adding new devices to the network.
- It is easy to troubleshoot and repair the network, as each device is connected to multiple other devices.
- The mesh topology is secure, as data can be transmitted between devices without passing through a central hub or switch.

Cons:

- The **mesh topology** is more expensive than other topologies, as it requires more cable and more devices.
- It is difficult to install and configure the network, as each device must be connected to multiple other devices.
- The mesh topology is not very scalable, as the number of connections between devices can become unmanageable as the number of devices on the network increases.

Mesh Topology

Pros:

- The **mesh topology** is the most reliable and fault-tolerant topology.
- It is easy to expand the network by adding new devices to the network.
- It is easy to troubleshoot and repair the network, as each device is connected to multiple other devices.
- The mesh topology is secure, as data can be transmitted between devices without passing through a central hub or switch.

Cons:

- The **mesh topology** is more expensive than other topologies, as it requires more cable and more devices.
- It is difficult to install and configure the network, as each device must be connected to multiple other devices.
- The mesh topology is not very scalable, as the number of connections between devices can become unmanageable as the number of devices on the network increases.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Outline

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Multiplexation

- Multiplexation is the process of combining multiple data streams into a single data stream.
- Multiplexation is used to increase the efficiency of data transmission over a network.
- There are several different types of multiplexation, including time-division multiplexation (TDM), frequency-division multiplexation (FDM), and code-division multiplexation (CDM).
- Multiplexation is used in many different types of networks, including telephone networks, computer networks, and satellite networks.
- Multiplexation is an important concept in computer networking, as it allows multiple devices to share a single network connection.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Conmutation

- Conmutation is the process of switching data from one input port to one or more output ports.
- Conmutation is used to route data through a network, such as a computer network or a telephone network.
- There are several different types of conmutation, including circuit switching, packet switching, and message switching.
- Conmutation is an important concept in computer networking, as it allows data to be transmitted between devices on a network.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Access Protocols

- Access protocols are used to control access to a network and manage the transmission of data between devices on the network.
- There are several different types of access protocols, including Ethernet, Wi-Fi, and Bluetooth.
- Access protocols are an important concept in computer networking, as they define how devices on a network communicate with each other.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Transmission Protocols

- Transmission protocols are used to transmit data between devices on a network.
- There are several different types of transmission protocols, including TCP/IP, HTTP, and FTP.
- Transmission protocols are an important concept in computer networking, as they define how data is transmitted between devices on a network.
- Transmission protocols are used in many different types of networks, including computer networks, telephone networks, and satellite networks.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Outline

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Transmision Control Protocol — TCP

- Transmission Control Protocol (TCP) is a connection-oriented protocol that is used to transmit data between devices on a network.
- TCP is part of the Internet Protocol Suite (IPS), which is a set of protocols that are used to transmit data between devices on the Internet.
- It is derivated of the OSI model and the Department of Defense Model (DoD).
- The TCP protocol structure is defined in RFC 793. RFC 793 is a Request for Comments document that is published by the Internet Engineering Task Force (IETF).

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Transmision Control Protocol — TCP

- Source Port: The port number of the sender.
- Destination Port: The port number of the receiver.
- Sequence Number: The sequence number of the first byte in the TCP segment.
- Acknowledgment Number: The sequence number of the next byte the sender expects to receive.
- Data Offset: The length of the TCP header in 32-bit words.
- Reserved: Reserved for future use.
- Flags: Flags used to control the TCP connection.
- Window Size: The size of the receive window.
- Checksum: Used to verify the integrity of the TCP segment.
- Urgent Pointer: Indicates the end of urgent data.
- Options: Optional fields that can be included in the TCP header.
- Padding: Padding used to ensure that the TCP header is a multiple of 32 bits.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Internet Protocol — IP

- Internet Protocol (IP) is a connectionless protocol that is used to transmit data between devices on a network.
- IP is part of the Internet Protocol Suite (IPS), which is a set of protocols that are used to transmit data between devices on the Internet.
- It is derivated of the OSI model and the Department of Defense Model (DoD).
- The IP protocol structure is defined in RFC 791. RFC 791 is a Request for Comments document that is published by the Internet Engineering Task Force (IETF).

Internet Protocol — IP

- Version: The version of the IP protocol being used.
- Header Length: The length of the IP header in 32-bit words.
- Type of Service: The type of service requested by the sender.
- Total Length: The total length of the IP packet (header and data).
- Identification: A unique identifier for the IP packet.
- Flags: Flags used to control the fragmentation of the IP packet.
- Fragment Offset: Fragment's offset within the original IP packet.
- Time to Live: The maximum number of hops the IP packet can take before being discarded.
- Protocol: The protocol used to transmit the data in the IP packet.
- Header Checksum: Used to verify the integrity of the IP header.
- Source Address: The IP address of the sender.
- Destination Address: The IP address of the receiver.
- Options: Optional fields that can be included in the IP header.
- Padding: Padding used to ensure that the IP header is a multiple of 32 bits.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

IPv4

Pros:

- IPv4 has been around for a long time and is thoroughly tested in various environments and scenarios. It is known to work well and is reliable.
- Since IPv4 has been in use for a long time, most devices and systems are compatible with it.
- IPv4 addresses are easier to remember and write down compared to IPv6 addresses.
- There is a massive existing infrastructure that supports IPv4. This includes routers, switches, and other networking equipment.
- There is a large amount of documentation, expert knowledge, and community support available for IPv4.

IPv4

Cons:

- Limited Address Space: IPv4 uses 32-bit addresses, which allows for approximately 4.3 billion unique addresses. This is not sufficient for the number of devices connecting to the internet today.
- No Built-in Security: IPv4 doesn't have built-in security features, making it more vulnerable to malicious activities.
- Manual Configuration: IPv4 often requires manual configuration or third-party services, which can lead to human error.
- No Quality of Service (QoS): IPv4 does not have a good Quality of Service (QoS), which can lead to packet loss, delays, and jitter in the network.
- Fragmentation: IPv4 packets can be fragmented, which can lead to lower performance and higher load on network devices.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

IPv6

Pros:

- Larger Address Space: IPv6 uses 128-bit addresses, which provides a significantly larger number of addresses compared to IPv4.
- Simplified Header: The IPv6 header has a simpler format, which can improve routing efficiency and performance.
- Improved Security: IPv6 includes built-in support for IPsec (Internet Protocol Security), which was only optional in IPv4.
- Better Support for Quality of Service (QoS): IPv6 has improved support for QoS, which can lead to better performance for real-time data like video and audio streams.
- Auto-Configuration: IPv6 supports auto-configuration, which can make setting up networks easier and more efficient.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

IPv6

Cons:

- Complexity: IPv6 addresses are longer and more complex than IPv4 addresses. This can make them harder to remember and work with.
- Transition: Transitioning from IPv4 to IPv6 can be complex and costly. It requires changes to network infrastructure and software.
- Compatibility: Not all devices and systems are compatible with IPv6. While this is improving, there are still many devices that only support IPv4.
- Limited Adoption: Despite its advantages, IPv6 adoption is still not widespread. This means that many services and websites are not accessible via IPv6.
- No Native Broadcast: IPv6 does not support native broadcast, which can be a disadvantage in some scenarios.

Key Differences between IPv4 and IPv6

- Address Space: IPv4 uses 32-bit addresses, allowing for approximately 4.3 billion unique addresses. In contrast, IPv6 uses 128-bit addresses, providing a significantly larger number of addresses.
- Header Structure: The IPv6 header has a simpler format than the IPv4 header, which can improve routing efficiency and performance.
- Security: IPv6 includes built-in support for IPsec (Internet Protocol Security), which was only optional in IPv4.
- Quality of Service (QoS): IPv6 has improved support for QoS, which can lead to better performance for real-time data like video and audio streams.

Key Differences between IPv4 and IPv6

- Configuration: IPv6 supports auto-configuration, which can make setting up networks easier and more efficient. In contrast, IPv4 often requires manual configuration or third-party services.
- Fragmentation: IPv4 packets can be fragmented, which can lead to lower performance and higher load on network devices. IPv6 has moved the fragmentation to the end nodes, reducing the load on the routers.
- Broadcast Messages: IPv4 supports broadcast messages, which are sent to all devices in a network. IPv6 no longer supports this feature and has replaced it with multicast and anycast messages.

Outline

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Thanks!

Questions?

Repo:

github.com/engandres/ud-public/main/tree/computer-networks

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS