1. Layered architecture models: reference models, layers, protocols, encapsulation, addressing

Layered architecture

- To reduce the design complexity when solving different problems we generally use layering technique, most networks are organized as a stack of layers or levels.

- The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.

- The purpose of each layer is to offer certain services to the higher layers while shielding those layers from the details of how the offered services are actually implemented.

The advantages of the layered architecture

- Using it, the unmanageable task of designing the complete network can be broken into several smaller, manageable design problems, namely, the design of the individual layers.
- Ease of protocol design, because the aim and the interfaces of a specific layer are clearly defined.
- Enables collaboration between different vendors.
- When the characteristics or technology of one layer is changing the other layers are not effected.
- It provides a generic language to describe the operation and characteristics of the network.
- Dividing network in layers make network administrators life easier. They can troubleshoot issue more quickly and effectually by looking in a layer that is causing issue rather than finding it in the entire network.

Protocol

- The rules and conventions used in conversation are collectively known as **protocol**.
- Every layer has one or more protocols.
- These protocols help layer *n* on one machine communicate with layer *n* on the other machine.
- A list of the protocols used by a certain system, one protocol per layer, is called a **protocol stack.**
- A set of layers and protocols is called a **network architecture**.

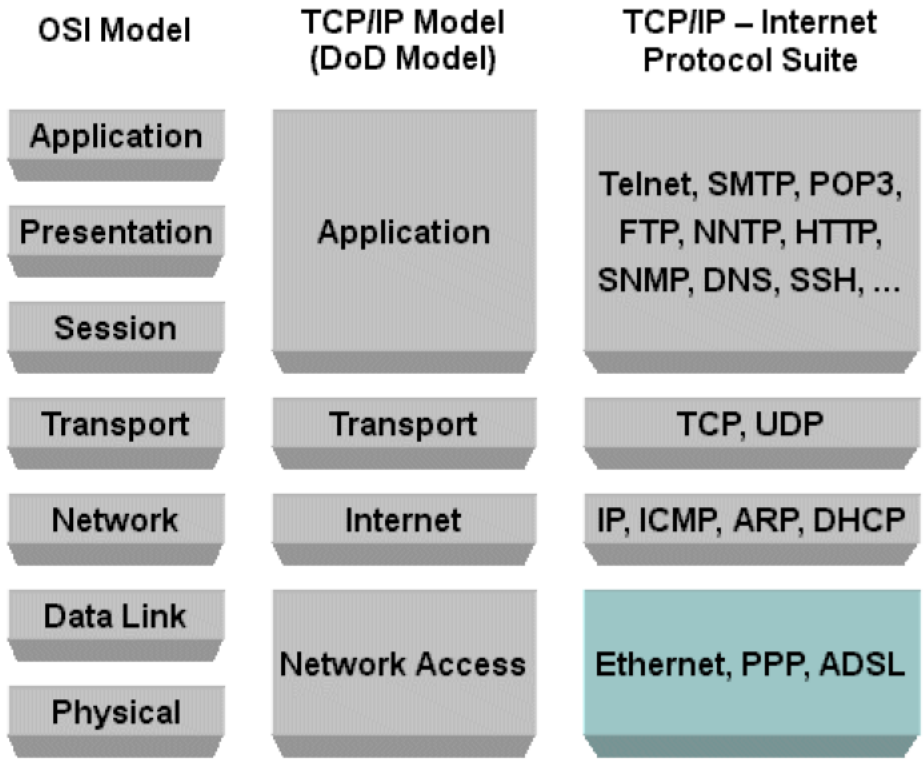
Rule Establishment (Cont.)

Protocols must account for the following requirements:

- An identified sender and receiver
- Common language and grammar
- Speed and timing of delivery
- Confirmation or acknowledgment requirements

TCP/IP

- Reference model of the ARPANET –research network of the DoD(Department of Defense)
- Later it became the TCP/IP model–1974 (Cerf, Kahn)
- First layered model of internetwork communication
- Describes the main four category of operation that is needed for successful communication.
- A TCP/IP protocols are fitted to this model
- Also called the Internet model



ISO Reference Model for Open System Interconnection(OSI)

- This model is based on a proposal developed by the International Standards Organization(ISO) as a first step toward international standardization of the protocols used in the various layers (Day and Zimmermann, 1983). It was revised in 1995 (Day).
- It describes what functions occur at each layer of the model that encourages industry standardization.
- Standardization of network components allows multiple-vendor development.
- It allows different types of network hardware and software to communicate.
- Each layer should perform a well-defined function
- The interface between the layers are well-defined and their implementation is independent from the other layers. It prevents changes in one layer from affecting other layers.
- Dividing network in layers make network administrators life easier. They can troubleshoot issue more quickly and effectually by looking in a layer that is causing issue rather than finding it in the entire network.

OSI –Application layer

- Application layer provides platform to send and receive data over the network. All applications and utilities that communicate with network fall in this layer. Examples:
    - File transfer
    - Email
    - HTTP

OSI –Presentation layer

- is concerned with the syntax and semantics of the information transmitted
- Converts the characters and numeric symbols to a standardized format.

- Compression, encryption

OSI –Session layer

- allows users on different machines to establish sessions between
- offer various services:
  - including dialog control,
  - token management,
  - synchronization,
  - checkpointing

OSI –Transport layer

- accept data from above it, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end
- isolates the upper layers from the inevitable changes in the hardware technology over the course of time.
- It sets up and maintains – when requested by the session layer - the connection between two devices.
- The transport layer is a true end-to-end layer; it carries data all the way from the source to the destination

OSI –Network layer

- Controls the communication subsystem
- Responsible for routing packets from source to destination
- Routes:
  - Wired(static)
  - Can be determined at the start of the conversation
  - Being determined for each packet - highly dynamic
- Congestion control
- Quality of service
- Billing based on traffic

OSI –Data link layer

- to transform a raw transmission facility into a line that appears free of undetected transmission errors. It does so by masking the real errors, so the network layer does not see them.
- breaks up the input data into data frames (typically a few hundred or a few thousand bytes) and transmit the frames sequentially and reliably
- Broadcast networks have an additional issue in the data link layer: how to control access to the shared channel. A special sublayer of the data link layer, the medium access control sublayer, deals with this problem.
- Flow control mechanism(fast trasnmitter–slow receiver problem)

OSI –Physical layer

- is concerned with transmitting raw bits over a communication channel
- electric voltages, radio frequencies, or pulses of infrared or ordinary light.
- Describes the type of the connectors, the functions of the wires and media
- Provides mechanical and electric interface according to the media.

Comparison of the OSI and TCP/IP Reference Models

Similarities:

1. They are both layered reference model. Both are based on the concept of a stack of independent protocols

2. The functionality of the layers is roughly similar and can be paired

Differences:

1. The following concepts are central to the OSI model:
   – Services
   – Interfaces
   – Protocols

2. The OSI reference model was devised before the corresponding protocols were invented. This ordering meant that the model was not biased toward one particular set of protocols, a fact that made it quite general.

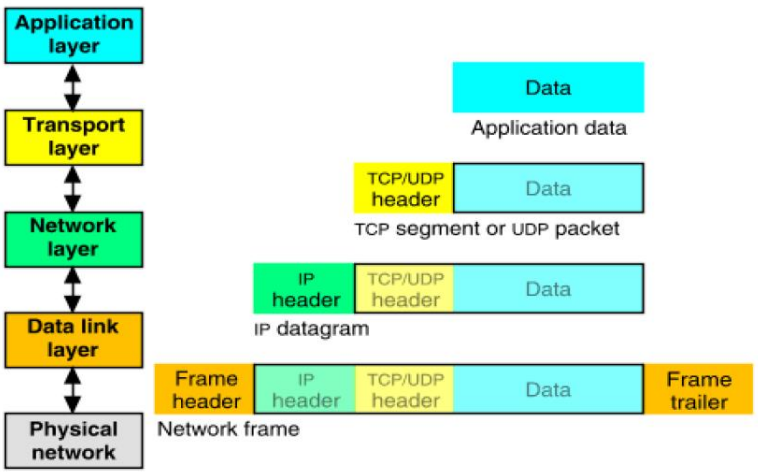
3. With TCP/IP the reverse was true: the protocols came first, and the model was really just a description of the existing protocols. There was no problem with the protocols fitting the model.

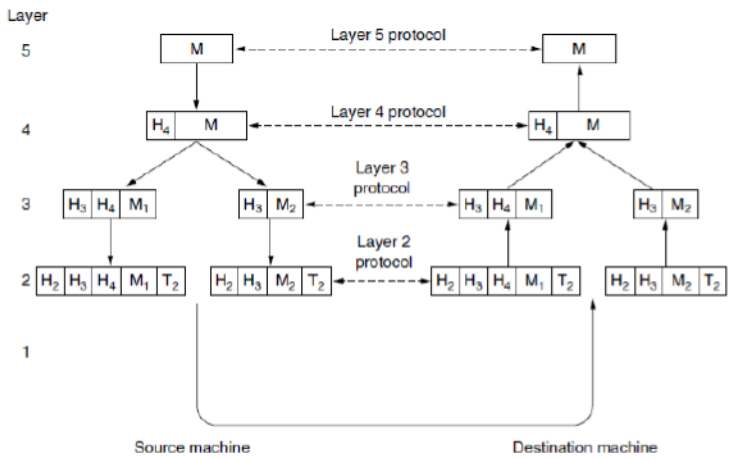
4. The number of the layers in the two models

5. Another difference is in the area of connectionless versus connection-oriented communication. The OSI model supports both connectionless and connection-oriented communication in the network layer, but only connection-oriented communication in the transport layer.

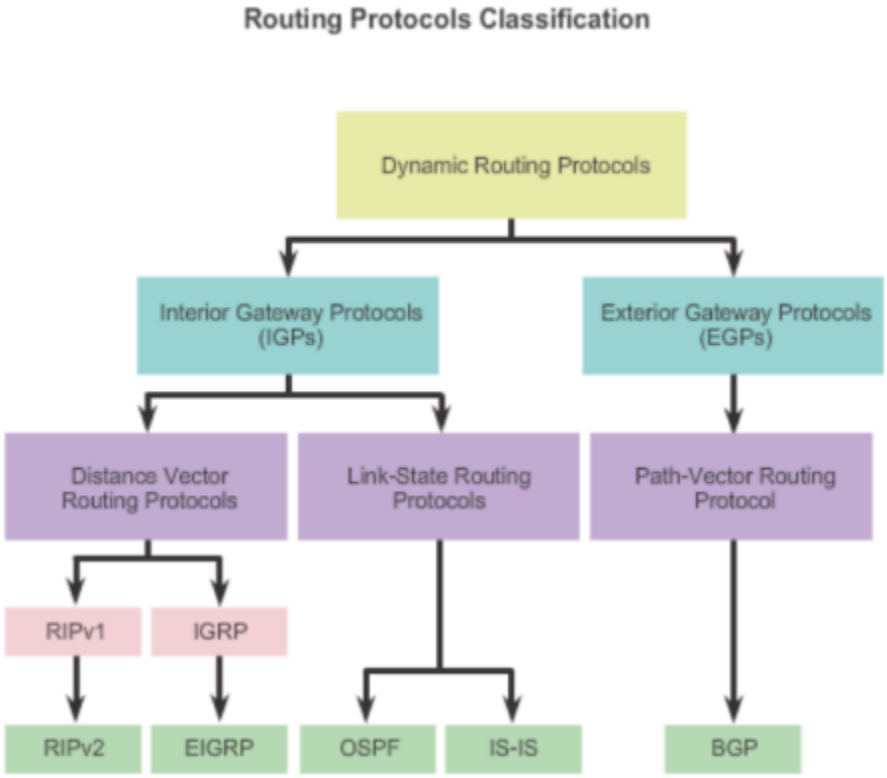
6. The TCP/IP model supports only one mode in the network layer (connectionless) but both in the transport layer, giving the users a choice.

Communication between peer layers, encapsulation





2. Routing: features, classification and operation of the different Interior Gateway Routing protocols, static routing, differences and similarities of DVR and LSR



Routing Protocols are used to facilitate the exchange of routing information between routers. The purpose of dynamic routing protocols includes:

- Discovery of remote networks
- Maintaining up-to-date routing information
- Choosing the best path to destination networks
- Ability to find a new best path if the current path is no longer available

Main components of dynamic routing protocols include:

- **Data structures** - Routing protocols typically use tables or databases for its operations. This information is kept in RAM.
- **Routing protocol messages** - Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and other tasks to learn and maintain accurate information about the network.
- **Algorithm** - Routing protocols use algorithms for facilitating routing information for best path determination.

Distance Vector

a simple routing protocol used in packet-switched networks that utilizes **distance** to decide the best packet forwarding path

Share updates between neighbors

- Not aware of the network topology

- Some send periodic updates to broadcast IP 255.255.255.255 even if topology has not changed
- Updates consume bandwidth and network device CPU resources
- RIPv2 and EIGRP use multicast addresses
- EIGRP will only send an update when topology has changed

Link-State Routing

A link-state routing protocol is like having a complete map of the network topology. The sign posts along the way from source to destination are not necessary, because all link-state routers are using an identical map of the network. A link-state router uses the link-state information to create a topology map and to select the best path to all destination networks in the topology.

Distance Vector	Link State
Lower bandwidth requirement, small packets, no flooding	More bandwidth, flooding and large link state packets
Local knowledge, routing table based on neighbours	Global knowledge, routing table is a complete map of the network
Bellman Ford algorithm	Dijkstra's algorithm
RIP / IGRIP	OSPF / ISIS
Best path based on hops	Best path based on cost
Low CPU	High CPU

Static Routing

S.NO	STATIC ROUTING	DYNAMIC ROUTING
1.	In static routing routes are user defined.	In dynamic routing, routes are updated according to topology.
2.	Static routing does not use complex routing algorithms.	Dynamic routing uses complex routing algorithms.
3.	Static routing provides high or more security.	Dynamic routing provides less security.
4.	Static routing is manual.	Dynamic routing is automated.
5.	Static routing is implemented in small networks.	Dynamic routing is implemented in large networks.
6.	In static routing, additional resources are not required.	In dynamic routing, additional resources are required.

Advantages	Disadvantages
Easy to implement in a small network.	Suitable only for simple topologies or for special purposes such as a default static route.
Very secure. No advertisements are sent as compared to dynamic routing protocols.	Configuration complexity increases dramatically as network grows.
Route to destination is always the same.	Manual intervention required to re-route traffic.
No routing algorithm or update mechanism required; therefore, extra resources (CPU or RAM) are not required.	

3. Routing: The features and operation of Distance Vector routing protocols, examples

The purpose of dynamic routing protocols includes:

- Discovery of remote networks
- Maintaining up-to-date routing information
- Choosing the best path to destination networks
- Ability to find a new best path if the current path is no longer available

Main components of dynamic routing protocols include:

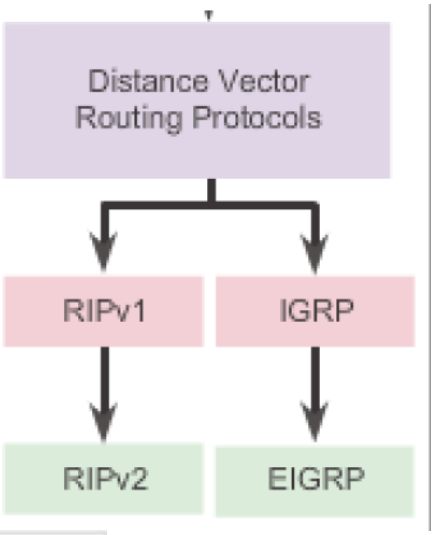
- **Data structures -** Routing protocols typically use tables or databases for its operations. This information is kept in RAM.
- **Routing protocol messages -** Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and other tasks to learn and maintain accurate information about the network.
- **Algorithm -** Routing protocols use algorithms for facilitating routing information for best path determination.

Distance Vector

a simple routing protocol used in packet-switched networks that utilizes **distance** to decide the best packet forwarding path

Share updates between neighbors

- Not aware of the network topology
- Some send periodic updates to broadcast IP 255.255.255.255 even if topology has not changed
- Updates consume bandwidth and network device CPU resources
- RIPv2 and EIGRP use multicast addresses
- EIGRP will only send an update when topology has changed



RIP uses the Bellman-Ford algorithm as its routing algorithm.

- computes shortest paths from a single source vertex to all of the other vertices in a weighted digraph

IGRP and EIGRP use the Diffusing Update Algorithm (DUAL) routing algorithm developed by Cisco.

- to ensure that a given route is recalculated globally whenever it might cause a routing loop

Routing Protocol	Metric
Routing Information Protocol (RIP)	• The metric is "hop count". • Each router along a path adds a hop to the hop count. • A maximum of 15 hops allowed.
Enhanced Interior Gateway Routing Protocol (EIGRP)	• It calculates a metric based on the slowest bandwidth and delay values. • It could also include load and reliability into the metric calculation.

4. Routing: The basic features and operation of Link State routing protocols, examples

A **link-state routing protocol** is like having a complete map of the network topology. The sign posts along the way from source to destination are not necessary, because all link-state routers are using an identical map of the network. A link-state router uses the link-state information to create a topology map and to select the best path to all destination networks in the topology.

1. Routers learn about their own links and their own directly connected networks.
2. Routers are responsible for meeting their neighbors on directly connected networks.
3. Routers build a link-state packet (LSP) containing the state of each directly connected link.
4. Routers flood the LSP to all neighbors, who then store all LSPs received in a database.
5. Routers use the database to construct a complete map of the topology and compute the best path to each destination network.

Advantages of link-state routing:

- Immediate flooding of link-state packets achieves faster convergence.
- LSPs are sent only when there is a change in the topology and contain only the information regarding that change.
- Hierarchical design used when implementing multiple areas.

Disadvantages of link-state routing:

- Maintaining a link-state database and a SPF tree requires additional memory.
- Calculating the SPF algorithm also requires additional CPU processing.
- Bandwidth can be adversely affected by link-state packet flooding.

The network is converged when all routers have complete and accurate information about the entire network:

- Convergence time is the time it takes routers to share information, calculate best paths, and update their routing tables. A network is not completely operable until the network has converged.
- Convergence properties include the speed of propagation of routing information and the calculation of optimal paths. The speed of propagation refers to the amount of time it takes for routers within the network to forward routing information.
- Generally, older protocols, such as RIP, are slow to converge, whereas modern protocols, such as EIGRP and OSPF, converge more quickly.

Open Shortest Path First (OSPF)	• The metric is "cost" which is the based on the cumulative bandwidth from source to destination. • Faster links are assigned lower costs compared to slower (higher cost) links.

OSPF gathers link state information from available routers and constructs a topology map of the network.

OSPF is widely used in large enterprise networks. IS-IS, another LSR-based protocol, is more common in large service provider networks.

Terminology of OSPF

OSPF – Open Shortest Path First, link-state routing protocol, using Dijkstra's algorithm
Operation of OSPF:

1. **Establish neighbor adjacencies**
    - OSPF-enabled routers must form adjacencies with their neighbor before they can share information with that neighbor.
    - An OSPF enabled router sends Hello packets out all OSPF-enabled interfaces to determine whether neighbors are present on those links.
    - If a neighbor is present, the OSPF enabled router attempts to establish a neighbor adjacency with that neighbor.
2. **Exchange link-state advertisements**
    - After adjacencies are established, routers then exchange link state advertisements (LSAs).
    - LSAs contain the state and cost of each directly connected link.
    - Routers flood their LSAs to adjacent neighbors. Adjacent neighbors receiving the LSA immediately flood the LSA to other directly connected neighbors, until all routers in the area have all LSAs.
3. **Build the topology table**
    - After the LSAs are received, OSPF-enabled routers build the topology table (LSDB) based on the received LSAs.
    - This database eventually holds all the information about the topology of the network.
    - It is important that all routers in the area have the same information in their LSDBs.
4. **Execute the SPF algorithm**
    - Routers then execute the SPF algorithm. The SPF algorithm creates the SPF tree.
5. **Build the routing table**

From the SPF tree, the best paths are inserted into the routing table. Routing decisions are made based on the entries in the routing table.

Single and multiarea OSPF

Single-Area OSPF

- If the routes are not summarized, the routing table can become very large.
- Each router must maintain detailed information about every network in the routing domain.

Multiarea OSPF

- Smaller routing tables
- Reduced link-state update overhead
- Reduced frequency of SPF calculations

OSPF uses a two-layer area hierarchy:

Backbone area, transit area or area 0

- Two principal requirements for the backbone area are that it must connect to all other nonbackbone areas and this area must be always contiguous; it is not allowed to have split up the backbone area.
- Generally, end users are not found within a backbone area.

Nonbackbone area

- The primary function of this area is to connect end users and resources.
- Nonbackbone areas are usually set up according to functional or geographic groupings.
- Traffic between different nonbackbone areas must always pass through the backbone area.

OSPF Router roles

ABR: A router that has interfaces connected to at least two different OSPF areas, including the backbone area. ABRs contain LSDB information for each area, make route calculation for each area and advertise routing information between areas.

ASBR: ASBR is a router that has at least one of its interfaces connected to an OSPF area and at least one of its interfaces connected to an external non-OSPF domain.

Internal router: A router that has all its interfaces connected to only one OSPF area.

Backbone router: A router that has at least one interface connected to the backbone area.

OSPF Packets

OSPF Routers Exchange Packets - These packets are used to discover neighboring routers and also to exchange routing information to maintain accurate information about the network.

Type 1: Hello packet:

- Discover OSPF neighbors and establish neighbor adjacencies.
- Advertise parameters on which two routers must agree to become neighbors.
- Elect the Designated Router (DR) and Backup Designated Router (BDR) on multiaccess networks like Ethernet and Frame Relay.

OSPF Hello packets are transmitted:

- To 224.0.0.5 in IPv4 and FF02::5 in IPv6 (all OSPF routers)
- Every 10 seconds (default on multiaccess and point-to-point networks)
- Every 30 seconds (default on non-broadcast multiaccess [NBMA] networks)
- Dead interval is the period that the router waits to receive a Hello packet before declaring the neighbor down
- Router floods the LSDB with information about down neighbors out all OSPF enabled interfaces

Type 2: Database Description (DBD) packet: When the OSPF neighbor adjacency is already established, a DBD packet is used to describe LSDB so that routers can compare whether databases are in sync.

Type 3: Link-State Request (LSR) packet: The router will send an LSR packet to inform OSPF neighbors to send the most recent version of the missing LSAs.

Type 4: Link-State Update (LSU) packet: LSU packets are used for the flooding of LSAs and sending LSA responses to LSR packets.

Type 5: Link-State Acknowledgment (LSAck) packet: LSAcks are used to make flooding of LSAs reliable.

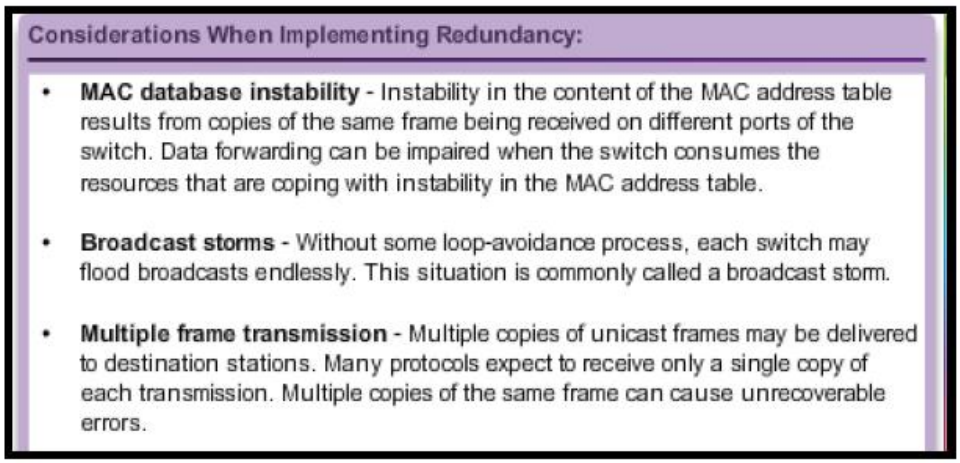
5. The role and implementation of redundancy in LAN environment (STP, Etherchannel, HSRP)

Redundancy:

Multiple cabled paths between switches:

- Provide physical redundancy in a switched network.
- Improves the reliability and availability of the network.
- Enables users to access network resources, despite path disruption.

Problems with Redundancy:



Goal of STP (Spanning-Tree Protocol)

To create a loop-free topolgy.

Operation of STP

- 1. Electing a designated switch called root Bridge
- 2. Apart from the root bridge choosing a root port on every switch
- 3. Choosing a port on each segment where the segment can be reached with the best path (Designated port)
- 4.Electing alternate (blocked) ports

How does the STA create a loop-free topology?

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

Port roles

- Root port: closest port to the root bridge

- Designated port: best path to receive traffic leading to the root bridge
- Alternate (Blocked) port: not a root or a designated port. Not turned on.

Rapid Spanning-Tree Protocol (RSTP)

- RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this

STP PortFast

- PortFast causes a switch or trunk port to enter the spanning tree forwarding state immediately, bypassing the listening and learning states

BPDU (Bridge Protocol Data Unit) guard

- Prevents accidental connection of switching devices to PortFast-enabled ports. Connecting switches to PortFast-enabled ports can cause Layer 2 loops or topology changes.

BPDU filtering

- Restricts the switch from sending unnecessary BPDUs out access ports

Purpose of link aggregation

- To increase bandwidth, redundancy
- To enable load-sharing
- To provide fault tolerance
- Without being blocked by STP
- ETHERCHANNEL

Operation and advantages of Etherchannel

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

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

- Most configuration tasks can be done on the EtherChannel interface instead of on each individual port, ensuring configuration consistency throughout the links.
- EtherChannel relies on existing switch ports.
- Load balancing takes place between links that are part of the same EtherChannel.
- EtherChannel creates an aggregation that is seen as one logical link. Where there is only one EtherChannel link, all physical links in the EtherChannel are active because STP sees only one (logical) link.
- EtherChannel provides redundancy because the overall link is seen as one logical connection. Additionally, the loss of one physical link within the channel does not create a change in the topology.

Limitations

- Interface types cannot be mixed. For example, Fast Ethernet and Gigabit Ethernet cannot be mixed within a single EtherChannel.

- Currently each EtherChannel can consist of up to eight compatibly-configured Ethernet ports. EtherChannel provides full-duplex bandwidth up to 800 Mbps (Fast EtherChannel) or 8 Gbps (Gigabit EtherChannel) between one switch and another switch or host.
- The Cisco Catalyst 2960 Layer 2 switch currently supports up to six EtherChannels.
- The individual EtherChannel group member port configuration must be consistent on both devices.
- Each EtherChannel has a logical port channel interface. A configuration applied to the port channel interface affects all physical interfaces that are assigned to that interface.

Protocols

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

First-Hop Redundancy

- Network hosts are configured with a single default gateway IP address
- If the router whose IP address serves as the default gateway to the network host fails, a network host will be unable to send packets to another subnet
- With first-hop router redundancy, a set of routers or Layer 3 switches work together to present the illusion of a single virtual router to the hosts on the LAN.
- By sharing an IP address and a MAC address, two or more routers can act as a single “virtual” router

HSRP

- When frames are to be sent from the workstation to the default gateway, the workstation uses ARP to resolve the MAC address that is associated with the IP address of the default gateway.
- The ARP resolution will return the MAC address of the virtual router.
- Frames that are sent to the MAC address of the virtual router can then be physically processed by an active router that is part of that virtual router group.
- The physical router that forwards this traffic is transparent to the network hosts.
- The redundancy protocol provides the mechanism for determining which router should take the active role in forwarding traffic and determining when that role must be taken over by a standby router.

When the forwarding router or a link to it fails

  - The standby router stops seeing hello messages from the forwarding router.
  - The standby router assumes the role of the forwarding router.
  - As the new forwarding router assumes both the IP and MAC addresses of the virtual router, the end stations see no disruption in service.

- HSRP active and standby routers send hello messages to multicast address 224.0.0.2 (all routers) for Version 1, or 224.0.0.102 for Version 2, using User Datagram Protocol (UDP) port 1985.
- Hello messages are used to communicate between routers in the HSRP group.
- All the routers in the HSRP group need to be L2 adjacent so that hello packets can be exchanged.

HSRP Router roles

All the routers in an HSRP group have specific roles and interact in specific manners:

Virtual router

- An IP and MAC address pair that end devices have configured as their default gateway.
- The active router processes all packets and frames sent to the virtual address.
- The virtual router processes no physical frames. There is one virtual router in an HSRP group.

Active router

- The active router physically forwards packets sent to the MAC address of the virtual router.
- There is one active router in an HSRP group.

Standby router

- Listens for periodic hello messages. When the active router fails, the other HSRP routers stop seeing hello messages from the active router.
- The standby router then assumes the role of the active router. There is one standby router in an HSRP group.

Other routers

- There can be more than two routers in an HSRP group, but only one active and one standby router is possible.
- The other routers remain in the initial state, and if both the active and standby routers fail, all routers in the group contend for the active and standby router roles.

Priority and preemptive operation

- Default priority is 100, and the router with the highest IP address is elected as the active router.
- Regardless of other router priorities or IP addresses, an active router will stay active by default.
- A new election will occur only if the active router is removed.
- When the standby router is removed, a new election is made to replace the standby router.
- This behavior can change with the preempt option.

Interface tracking with HSRP

- HSRP has a built-in mechanism for detecting link failures and starting the HSRP reelection process.
- When a tracked interface becomes unavailable, the HSRP priority of the router is decreased.
- When properly configured, the HSRP tracking feature ensures that a router with an unavailable key interface will relinquish the active router role.
- When the conditions that are defined by the object are fulfilled, the router priority remains the same. Else, it is decremented.
- The amount of decrease can be configured. The default value is 10.

HSRP timers

- By default, the HSRP hello time is 3 seconds, and the hold time is 10 seconds, which means that the failover time could be as much as 10 seconds for clients to start communicating with the new default gateway.
- In some cases, this interval may be excessive for application support.
- The hello-time and the hold-time parameters are configurable.

6. Data Link Layer services and tasks, Media access control types, Ethernet

Functions of the Data Link layer:

The data link layer uses the services of the physical layer to send and receive bits over communication channels. It has a number of functions, including:

- Providing a well-defined service interface to the network layer.
- The sender takes the packets it gets from the network layer and encapsulates them into frames for transmission.
- must deliver packets to the destination network layer in the same order they were passed to the data link layer on the sending machine
- Dealing with transmission errors.
- Regulating the flow of data so that slow receivers are not swamped by fast senders.
- Addressing
- Link management

Error control:

- It must be noticed with the highest probability if the received message includes some errors.
- If the receivers notices that an error occured during transmission, a mechanism is needed to recover from this situation
- Two basic strategies:
    - Error-correcting:

      The transmitted frame includes enough redundant information to enable the receiver to deduce the original data -> unreliable channels(wifi)

    - Error detecting and retransmission request:

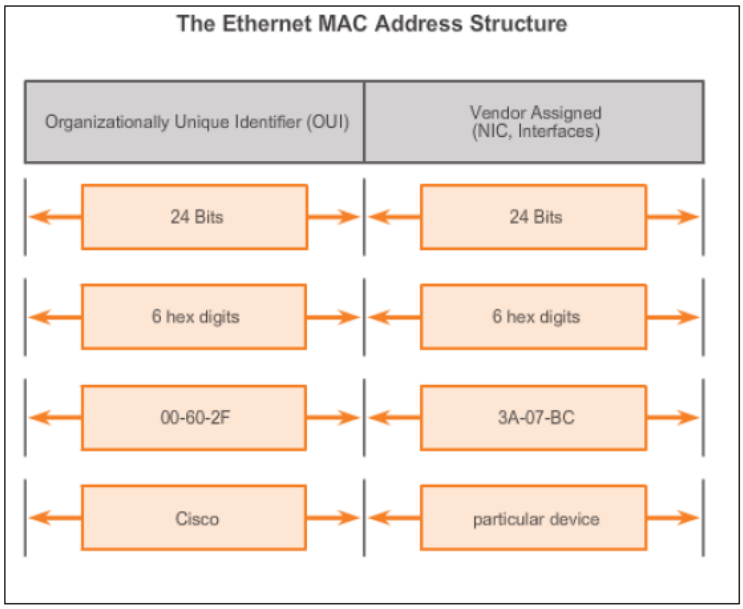
      The transmitted frame includes only enough redundancy to allow the receiver to deduce that an error has occurred (but not which error). The faulty frame is retransmitted. -> reliable channels(optical)
- Error control is based on retransmission. Faulty frames are not acknowledged, or negative acknowledgment is sent. The sender is notified from the negative ack or the lack of acks that the frame was not delivered or delivered correctly.

- Error correcting codes(FEC –Forward error correction)
    - Hamming codes.
    - Binary convolutional codes.
    - Reed-Solomon codes.
    - Low-Density Parity Check codes.

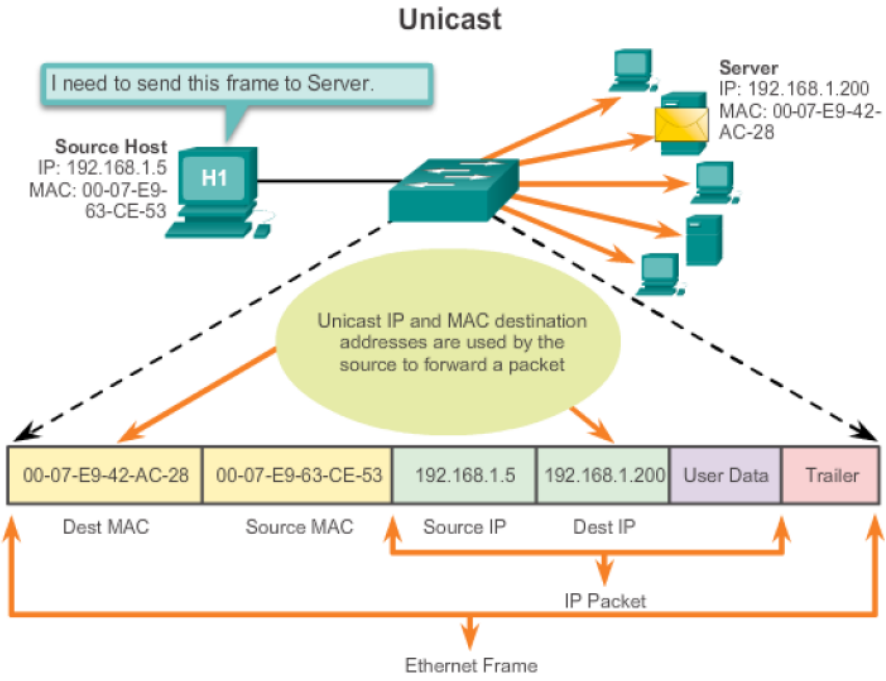
- Error detecting codes
    - Parity.
    - Checksums.
    - Cyclic Redundancy Checks (CRCs).

Addressing:

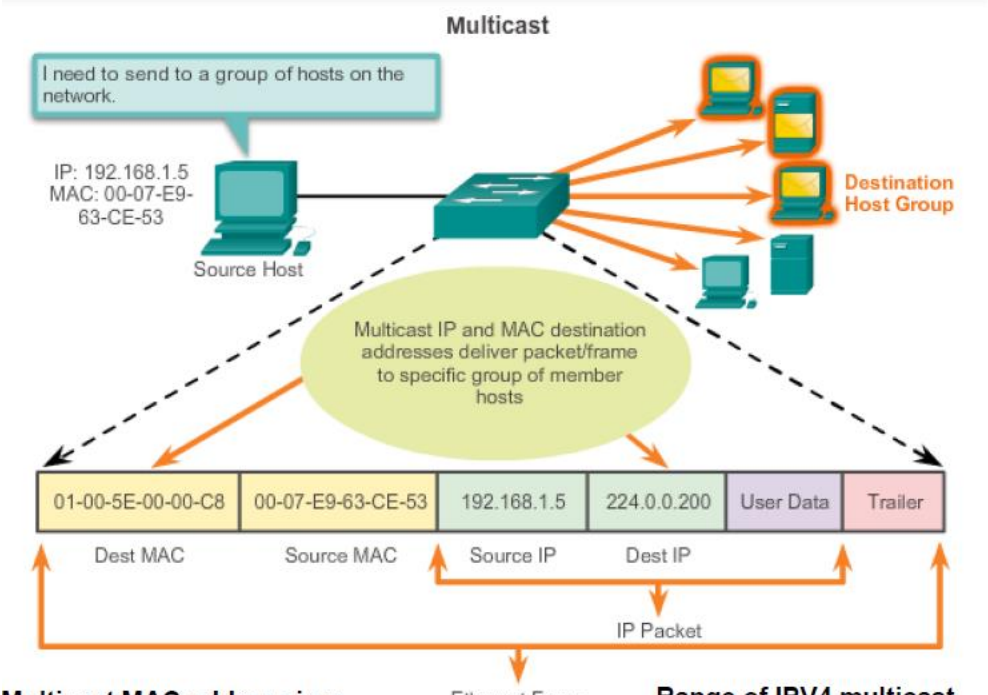
MAC-address



Unicast MAC Address



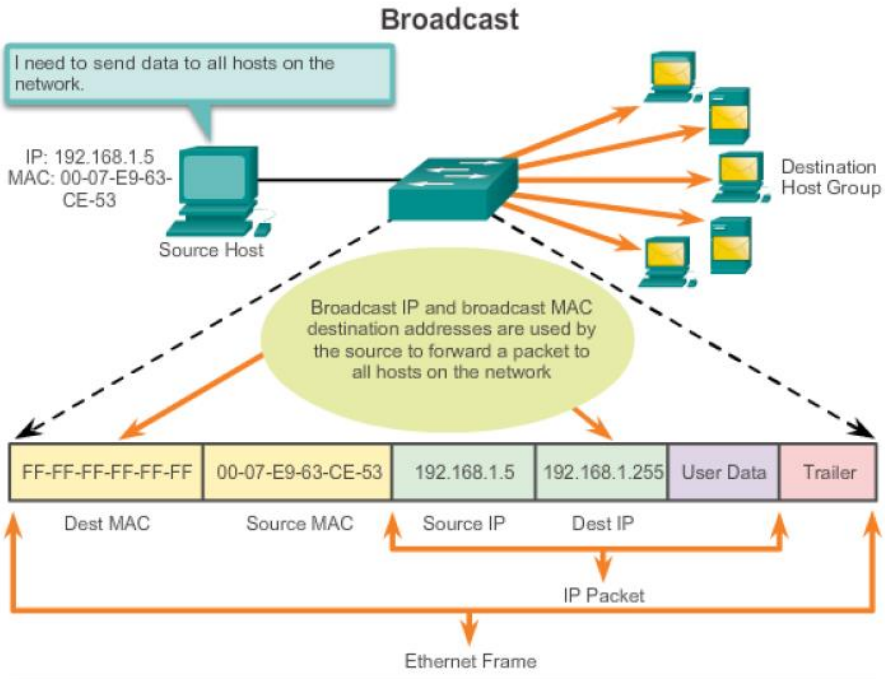
Multicast MAC Address



Multicast MAC address is a special value that begins with 01-00-5E in hexadecimal

Range of IPV4 multicast addresses is 224.0.0.0 to 239.255.255.255

Broadcast MAC Address



Ethernet Protocol:

- Most widely used LAN technology
- Operates in the data link layer and the physical layer
- Family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards
- Supports data bandwidths of 10, 100, 1000, 10,000, 40,000, and 100,000 Mbps (100 Gbps)

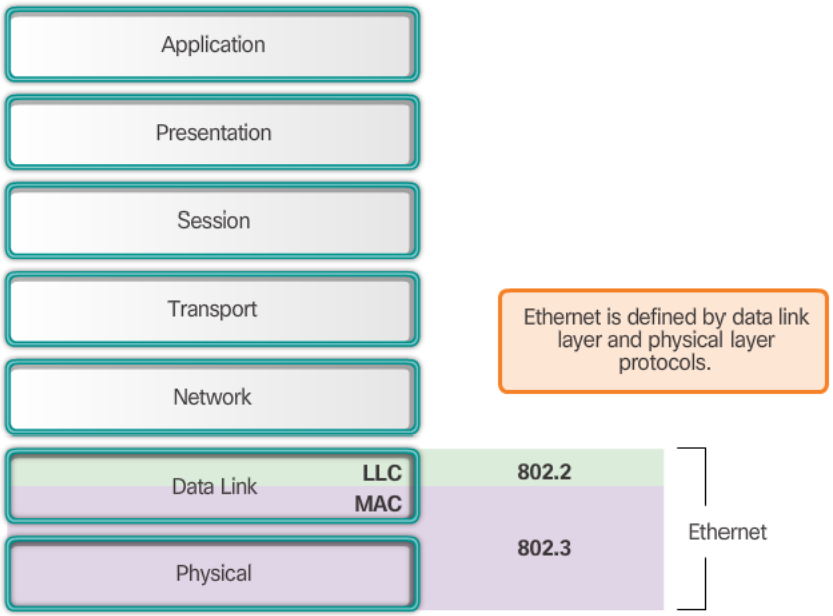
Ethernet standards:

- Define Layer 2 protocols and Layer 1 technologies
- Two separate sub layers of the data link layer to operate -Logical link control (LLC) and the MAC sublayers

Ethernet II Frame Structure and Field Size

Ethernet II					
8 Bytes	6 Bytes	6 Bytes	2 Bytes	46 to 1500 Bytes	4 Bytes
Preamble	Destination Address	Source Address	Type	Data	Frame Check Sequence

Ethernet Encapsulation

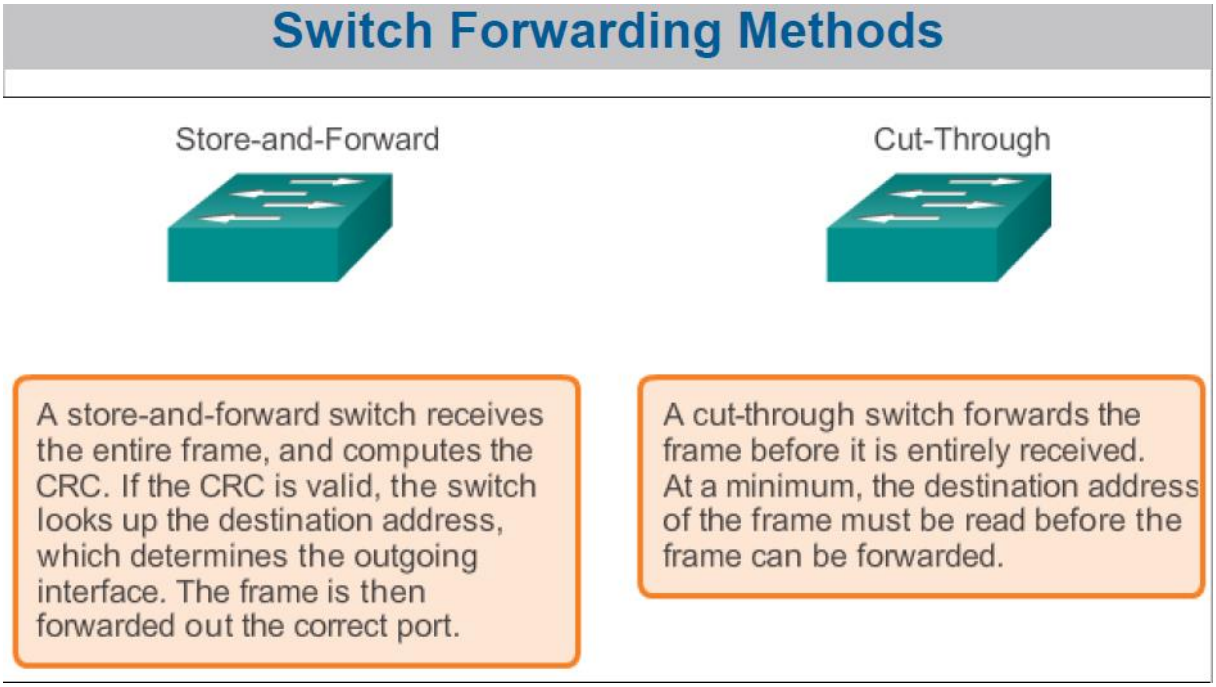


7. Switching: Switched LAN environment, Switch operation, VLANs, DTP, VTP

Switching as a General Concept

- A switch makes a decision based on ingress and a destination port.
- A LAN switch keeps a table that it uses to determine how to forward traffic through the switch.
- Cisco LAN switches forward Ethernet frames based on the destination MAC address of the frames.

Switch modes



- Cut Through
  - Allows the switch to start forwarding in about 10 microseconds
  - No FCS check
  - No automatic buffering

Dynamically Populating a Switch MAC Address Table

- A switch must first learn which devices exist on each port before it can transmit a frame.
- It builds a table called a MAC address or content addressable memory (CAM) table.
- The mapping device <-> port is stored in the CAM table.
- CAM is a special type of memory used in high-speed searching applications.
- The information in the MAC address table used to send frames.
- When a switch receives an incoming frame with a MAC address that is not found in the CAM table, it floods it to all ports, but the one that received the frame.

ARP Table

- Used to find the MAC address that is mapped to the destination IPv4 address.
- If the destination IPv4 address is on the same network as the source IPv4, the device will search the ARP table for the destination IPv4 address.
- If the destination IPv4 address is on a different network, the device will search for the IPv4 address of the default gateway.
- If the device locates the IPv4 address, its corresponding MAC address is used as the destination MAC address in the frame.
- If no entry is found, then an ARP request is sent.

VLAN Definitions

- A VLAN is a logical partition of a Layer 2 network.
- Multiple partitions can be created, allowing for multiple VLANs to co-exist.
- Each VLAN is a broadcast domain, usually with its own IP network.
- VLANs are mutually isolated and packets can only pass between them via a router.
- The partitioning of the Layer 2 network takes place inside a Layer 2 device, usually via a switch.
- The hosts grouped within a VLAN are unaware of the VLAN's existence.

Operation

Virtual Local Area Networks (**VLANs**) separate an existing physical network into multiple logical networks. Thus, each **VLAN** creates its own broadcast domain. Communication between two **VLANs** can only occur through a router that is connected to both

Types of VLANs

- Data VLAN: carry only user-generated traffic
- Default VLAN: default vlan is VLAN 1.
- Native VLAN: 802.1Q trunk port places untagged traffic on the native VLAN.
    - VLAN 99
- Management VLAN: any VLAN you configure to access the management capabilities of a switch

Benefits of VLANs

- Security
- Cost reduction
- Better performance
- Shrink broadcast domains
- Improved IT staff efficiency

VLAN Trunks

- A VLAN trunk carries more than one VLAN.
- A VLAN trunk is usually established between switches so same-VLAN devices can communicate, even if physically connected to different switches.
- A VLAN trunk is not associated to any VLANs; neither is the trunk ports used to establish the trunk link.
- Cisco IOS supports IEEE 802.1q, a popular VLAN trunk protocol.

Dot1Q:

IEEE **802.1Q**, often referred to as Dot1q, is the networking standard that supports virtual LANs (VLANs) on an IEEE 802.3 Ethernet network. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames

- Frame tagging is the process of adding a VLAN identification header to the frame.

Dynamic Trunking Protocol

Networking protocol developed by Cisco Systems for the purpose of negotiating trunking on a link between two VLAN-aware switches, and for negotiating the type of trunking encapsulation to be used

Option	Description
access	Permanent access mode and negotiates to convert the neighboring link into an access link
dynamic auto	Will becomes a trunk interface if the neighboring interface is set to trunk or desirable mode
dynamic desirable	Actively seeks to become a trunk by negotiating with other auto or desirable interfaces
trunk	Permanent trunking mode and negotiates to convert the neighboring link into a trunk link

VTP

- Automates the propegation of VLAN information, such as additions, deletions and name changes
- Switches sycnhronize their configuration based on the received information
- Works based on clients and servers, servers can edit vlans, send advertisements, and save the configuration
- VTP messages are sent as multicast, every time there is a change or every 5 minutes by default
- VTP Pruning can help prevent flooding unneccesarry traffic to switched that do not have members in the specific VLANs
- VTP domains can be protected by configuring a VTP password, which is propagated in the domain in summary advertisments

8. Network Layer services and tasks, IP, IPv6, structure and operation of the routers

Functions of the network layer

- Network Service
- Addressing
- Routing
- Quality of Service: QoS:
- Maximum PDU (packet): **Maximum Transmission Unit**
- Flow and congestion control:
- Error reporting

Network Service

- Packets transmission from source to destination through more intermediary devices.
- The service must be independent from the router and the technology used in subnetworks.
- Transport layer should be shielded from the number, type and topology of the routers, networks.
- The network addresses made available to the transport layer should use a uniform numbering plan even across diffrerent LANs and WANs.

Addressing

- The address used in the network layer must uniquely identify the host on the whole network
- Physical addresses cannot be used for addressing the whole network
- Physical and network addresses are used together
- Physical address is used for medium access (Ethernet address), network addresses are used for addressing on the whole network (IP address)
- All interfaces on a router should posses physical address

Routing

- If communicating host were on the same segment of the network physical address would be sufficient
- In all other cases the network address identifies the peers in the communication.
- Network packets should be some how routed.
- The network address is not sufficient for routing the packets to a remote network
- The transmitted packet should be sent with the network address of the remote host together with the physical address of the router on the same segment.
- The router then forwards the packet to the physical address of the destination host or to the physical address of the next router.

Quality of Service: QoS

- QoS: parameters that describe the performance of the expected service
- Include
    - Bitrate(bandwidth)
    - Delay, jitter
    - Cost
    - Error rate

Maximum Transmission Unit

- Each network imposes some maximum size on its packets
- The factors contributing to the size of Maximum Transmission Unit (MTU)
    - Hardware (size of an Ethernet frame)
    - Operating systems (size of the buffers)

    - Protocols (number of bits in packet lentgh field)
    - Compliance with some (inter)national standard
    - Overhead – the amount of information added to the payload
    - Desire to prevent one packet from occupying the channel too long
- Transport layer usually fragments the data for transmission
- The network layer may further fragment this packet according to the different network types and at reception it reassembles the packets again.

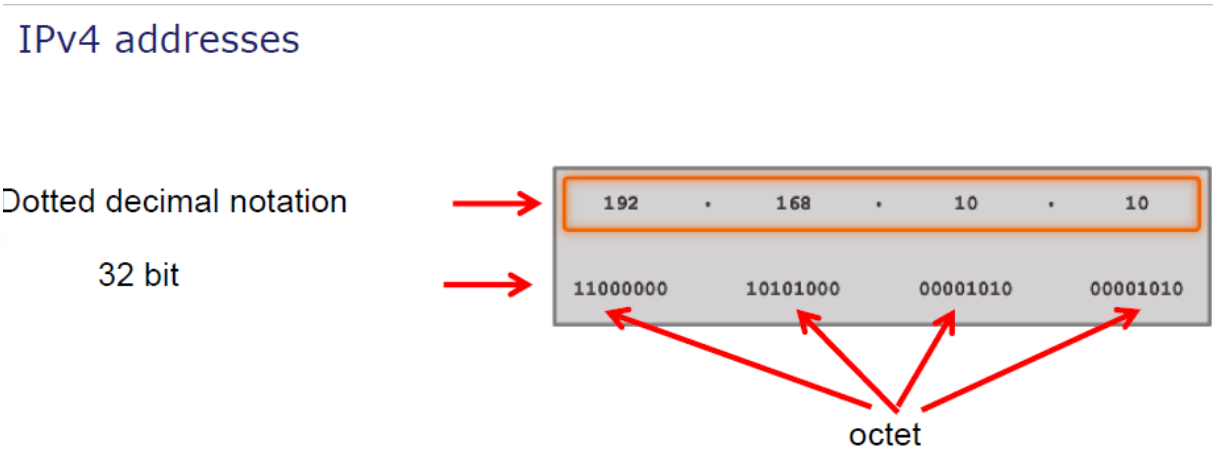
Flow and congestion control

- Flow control mechanism controls the traffic between host with different load and processing speed.
- Too many packets in (a part of) the network causes packet delay and loss that degrades performance. The load is greater than the resources can handle. This situation is called congestion. Congestion control means to recover from congestion.

The characteristics of the IP protocol:

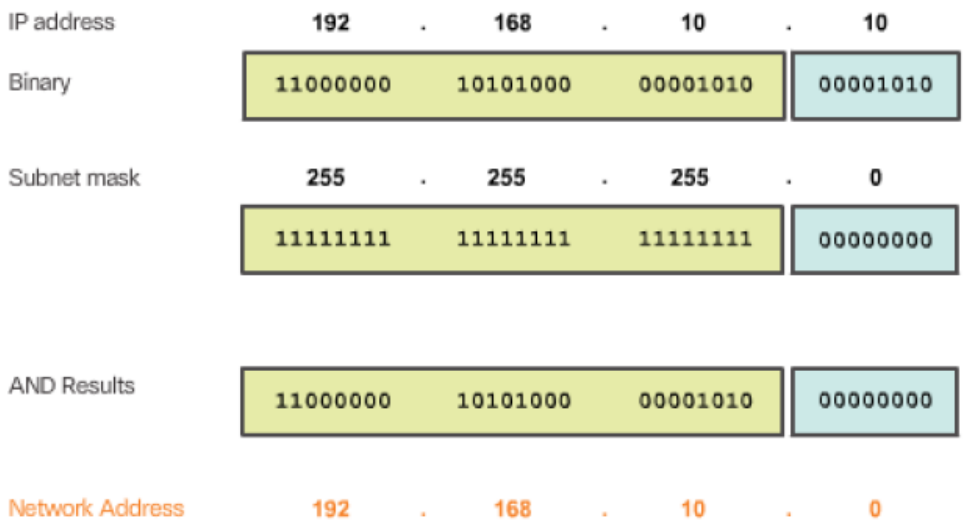
- Connectionless – does not set up a connection before data transmission the packets are forwarded independently from each other, on different routes maybe
- Unreliable – the packets can be damaged, lost, duplicated, delayed, and can arrive in wrong order
- There is no way for error correction, upper layer should deal with this problem: TCP, application layer
- best effort – The network does its best to deliver the packets, but it is not guaranteed.
- Medium independent – It forwards packets independently from the physical media.

Addressing:

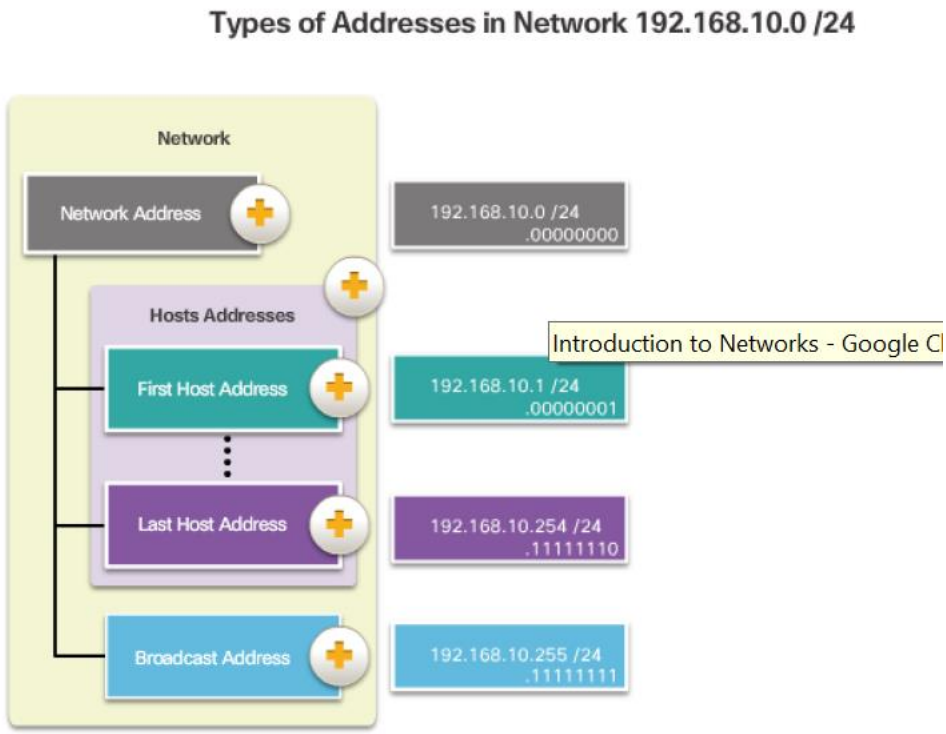


- Subnet mask - Used to identify the network/host portion of the IPv4 address. IPv4 address is logically AND-ed, bit by bit, with the subnet mask.
- Comparing the IP Address and the Subnet Mask
- The 1s in the subnet mask identify the network portion while the 0s identify the host portion.

Structure of addresses



Address Types



Multicast Addresses:

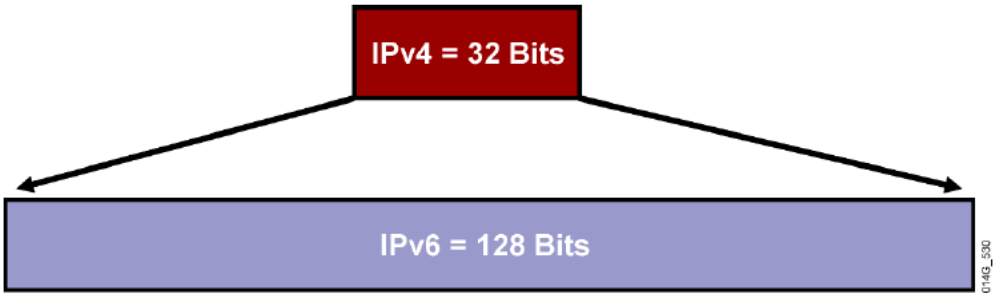
- A host sends a single packet to a selected set of hosts that subscribe to a multicast group.
- The 224.0.0.0 to 239.255.255.255 range of addresses are reserved for multicast.

Private Addresses:

- 10.0.0.0/8 or 10.0.0.0 to 10.255.255.255
- 172.16.0.0 /12 or 172.16.0.0 to 172.31.255.255
- 192.168.0.0 /16 or 192.168.0.0 to 192.168.255.255

Special Use IPv4 Addresses:

- Network addresses and Broadcast addresses – the first and the last IP addresses
- Loopback addresses 127.0.0.0/8 or 127.0.0.1 to 127.255.255.254
- Link-Local addresses or Automatic Private IP Addressing (APIPA) addresses169.254.0.0 /16 or 169.254.0.1 to 169.254.255.254
- TEST-NET addresses192.0.2.0/24 or 192.0.2.0to 192.0.2.255
- Experimental addresses – 240.0.0.0 - 255.255.255.254



IPv6 goals

- Give addressing possibilities for milliards of hosts
- Decrease the size of the IP routing table → faster forwarding
- Simplified protocol → faster processing
- Stronger security
- Differentiated services to different type of traffic

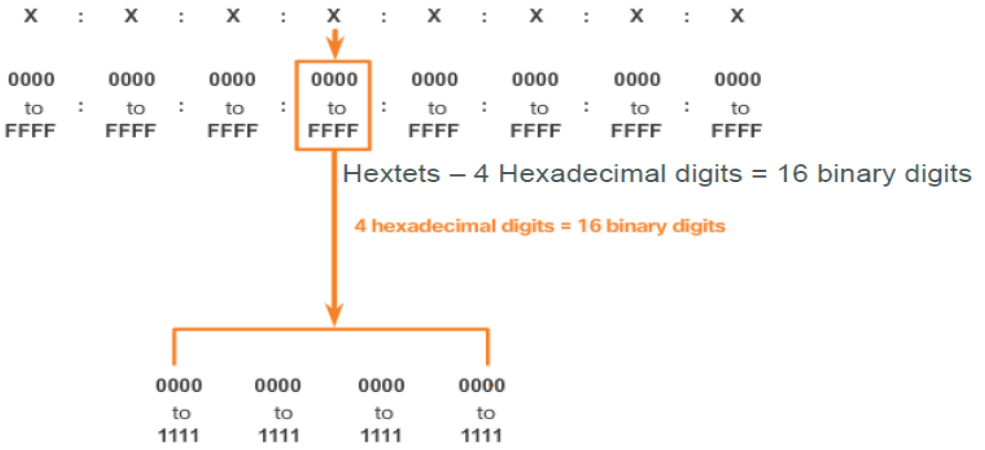
IPv6 functions

- Addressing the hosts
  - DHCP, stateful and stateless autoconfiguration (Stateless auto-configuration)
- Address aggregation
  - Large IPv6 address ranges enable IP address – blocks to be aggregated, which makes routing more efficient
- NAT/PAT is not needed anymore
- No broadcast
  - IPv6 does not use 3. layer broadcast messages instead multicast is used.
- More methods that support migration form IPv4 to IPv6

Address Representation

IPv6 Address Representation

- 128-bit hexadecimal format (0-9, A-F)
- Uses 16-bit hexadecimal number fields separated by colons (:)
- Every 4-hexadecimal digits are equivalent to 16-bits. Hextet
- Consists of 8 hextets/quartets which is the equivalent to 16-bits per-hextet.



Address Structure:

IPv6 Addressing Structure

Network prefix

- Prefix in IPv6 can be specified only with the number of bits
- CIDR or prefix notation

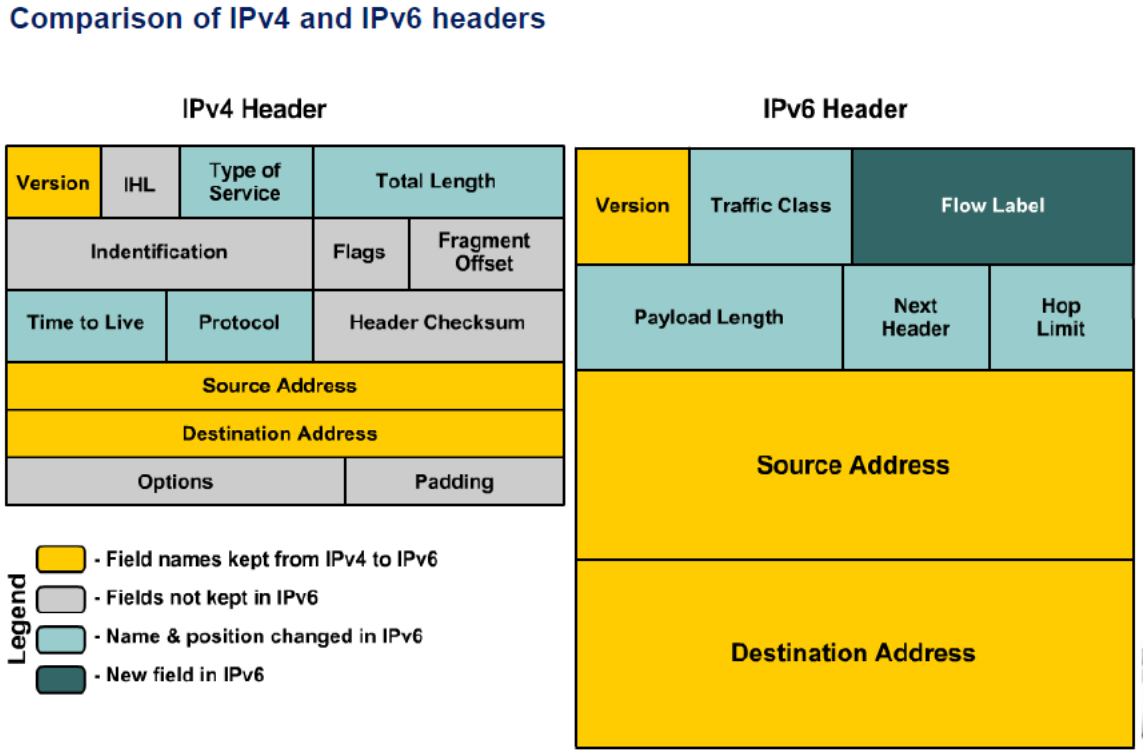
```
3ffe:1944:100:a::/64
16   32   48   64 bits
```

Types of IPv6 Addresses

- Unicast Address
  - Uniquely identifies a single interface on an IPv6 device.
  - A packet sent to a unicast address destination travels from one host
- Link-Local Address
  - Link-Local address are designed for use on a single local link.
  - Link-Local address are automatically configured on all interfaces.
  - The prefix used for a Link-Local address is FE80::X/10.
  - 1111 1110 1000 0000 (FE80) -1111 1110 1011 1111(FEBF)
- Loopback Address
  - Similar function to IPv4 127.0.0.1 address
  - The Loopback address is 0:0:0:0:0:0:0:1 or may be simplify by using double colons as ::1.
  - It is used by a device to send a packet to itself
- Multicast Address
  - A Multicast address identifies a group of interfaces.

    - All Multicast address are identified by their reserved address range FF00::0/8
    - A packet sent to a multicast address is delivered to all devices that are identified by that address.
- Anycast Address
    - A unicast address can be assigned to several interfaces/devices.
    - A packet sent to an Anycast address goes only to the nearest member of the group, according to the routing protocols measures of distance.
    - Anycastis described as a cross between a Unicast and Multicast.
    - The difference between an Anycastand Multicast is that in Anycastpacket is only delivered to a single device, while Multicast send it to multiple devices.

Comparison of IPv4 – IPv6



Thefields in the IPv6 packet header include:

- Version - This field contains a 4-bit binary value set to 0110 that identifies this as an IP version 6 packet.
- Traffic Class - This 8-bit field is equivalent to the IPv4 Differentiated Services (DS) field.
- Flow Label - This 20-bit field suggests that all packets with the same flow label receive the same type of handling by routers.
- Payload Length - This 16-bit field indicates the length of the data portion or payload of the IPv6 packet.
- Next Header - This 8-bit field is equivalent to the IPv4 Protocol field. It indicates the data payload type that the packet is carrying, enabling the network layer to pass the data to the appropriate upper-layer protocol.
- Hop Limit - This 8-bit field replaces the IPv4 TTL field.
- Source Address -This 128-bit field identifies the IPv6 address of the sending host.
- Destination Address - This 128-bit field identifies the IPv6 address of the receiving host.

9. Transport layer services and tasks, TCP, UDP characteristics and operation

Characteristics of the transport layer

- It is the center of the hierarchical model: provides data transmission independently from the lower layers ➔ End-to-end service

The main tasks of the transport layer

- Addresses – sockets and ports
- Connection establishment, maintain and tear
- Error handling
- Flow and congestion control
- Multiplexing between the different applications

Establishment, maintaining and tear down connections

Problem: unreliable network services (duplicated, delayed or lost packets)

- Unique segment identifier
- Limit the packet lifetime
  - Restricted network design
  - Hop count
  - Timestamps
- Three-way handshake
- Disconnect: symmetric and asymmetric
  - Problem: dataloss

Error handling

- Error detecting codes (checksum or CRC)
- Acknowledgement
- Limiting the number of sent and unacknowledged messages
- Sliding window

Flow control

- Congestion control
- To send packets more slowly
- To control the transmission rate
- Sliding window

Connectionless – UDP

Packets are injected into the network individually and routed independently from each other.

Connection oriented – TCP

A path from the source all the way to the destination must be established. That path is used for all traffic flowing over the connection.

Ports and sockets

It is needed to determine which local process at a given host actually communicates with which process, at which remote host, using which protocol.

Well-known ports:

- Belong to Standard servers : 1-1023
- E.g.: Telnet port = 23
- Most servers require only a single port.

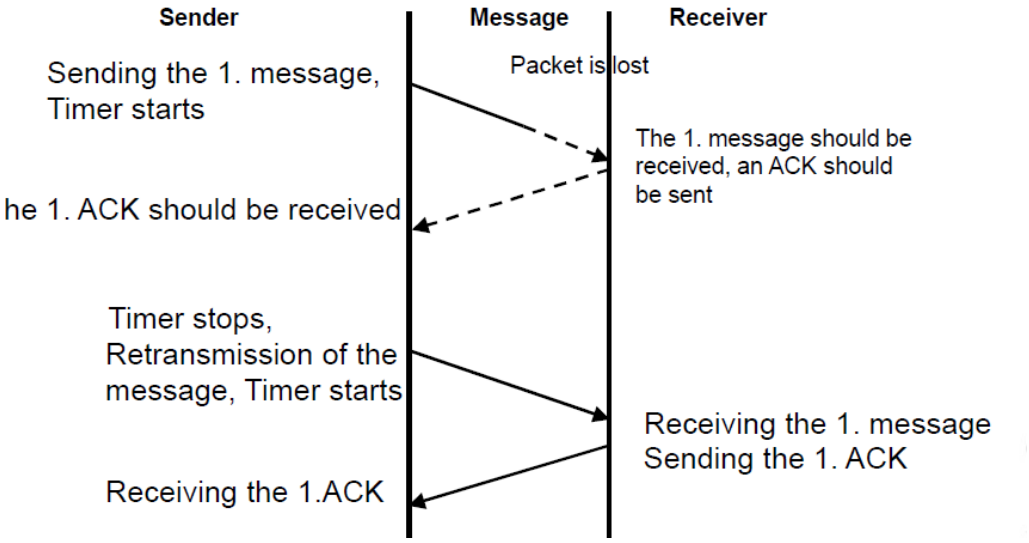
- FTP server, which uses two: 20 and 21
- Ephemeral port numbers have values greater than 1023, normally in the range of 1024 to 65535

Transmission Control Protocol

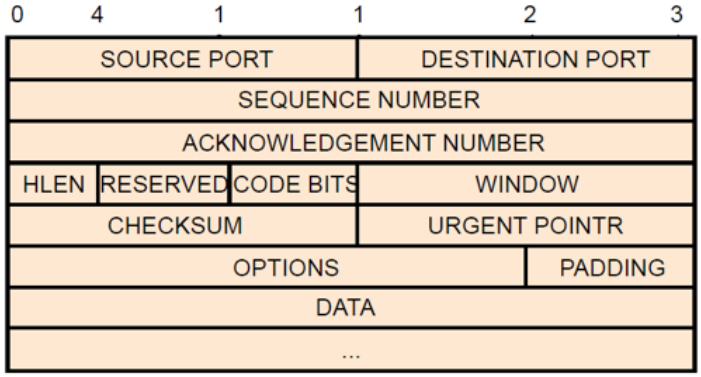
- RFC 793
- a reliable end-to-end byte stream over an unreliable internetwork
- Transport Layer protocol
- Applications that move large amount of data is not appropriate to use the unreliable services that are provided by IP and UDP
- Not a best practice to implement error handling in all Application Layer protocol
- It is needed to provide a Reliable data transmission protocol

To ensure reliability

- Positive acknowledgement with retransmission, PAR
- At the receiver node the protocol software sends an acknowledgement(=ACK) about receiving data.
- The sender stores a record for every sent message and waits for the ACK
- The Acknowledgment number points to the next byte of the message



The format of the TCP segment



Ports, connections and endpoints

- TCP enables that more applications simoultaneously communicate and the message is sent to the appropriate application.
- TCP also uses the protocol port numbers to address the end point of the message.
- The TCP port alone does not uniquely identify the destination object.
- Tcp uses the concept of connection for identification.
- Two end points identificate the connection. E.g.:
  (192.190.173.37, 25) and (192.190.173.55, 1071)
  Another connection on the same machine
  (192.190.173.37, 25) and (192.190.173.55, 1156)
- It is enough when there is one difference between the two times four identification numbers.

UDP Low Overhead versus Reliability

- UDP is a simple protocol.
- UDP provides the basic transport layer functions.
- UDP has much lower overhead than TCP.
- UDP is not connection-oriented and does not offer the sophisticated retransmission, sequencing, and flow control mechanisms.
- Applications running UDP can still use reliability, but it must be implemented in the application layer.
- However, UDP is not inferior.It is designed to be simpler and faster than TCP at the expense of reliability.

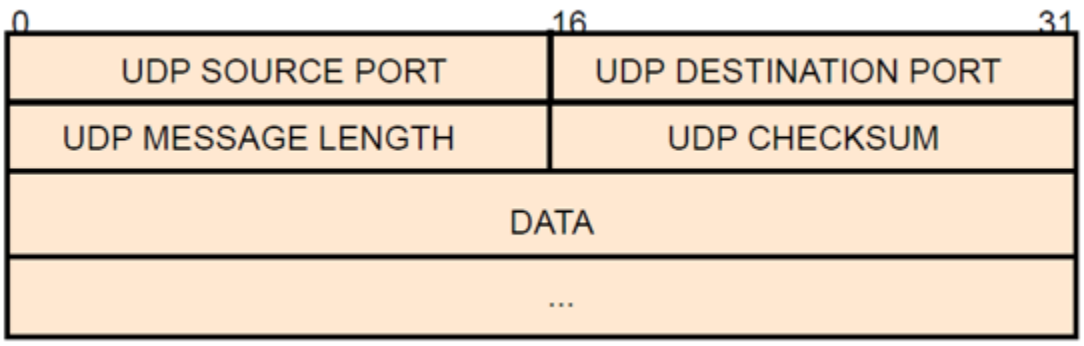
UDP Datagram Reassembly

- 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 in which it was received.
- The application must identify the proper sequence, if necessary.

UDP Server Processes

- UDP client-server communication is also initiated by a client application.
- The UDP client process dynamically selects a port number and uses this as the source port.
- The destination port is usually the well-known or registered port number assigned to the server process.
- The same source-destination pair of ports is used in the header of all datagrams used in the transaction.
- Data returning to the client from the server uses a flipped source and destination port numbers in the datagram header.

UDP message structure



10. The goal, role and methods of QoS techniques

The aspects of Quality of Service

- What applications need from the network?
- How to regulate the traffic that enter the network?
- How to reserve resources at routers that enters the network?
- Whether the network can safely accept traffic?

Application	Bandwidth	Delay	Jitter	Loss
Email	Low	Low	Low	Medium
File sharing	High	Low	Low	Medium
Web access	Medium	Medium	Low	Medium
Remote login	Low	Medium	Medium	Medium
Audio on demand	Low	Low	High	Low
Video on demand	High	Low	High	Low
Telephony	Low	High	High	Low
Videoconferencing	High	High	High	Low

Network Traffic Trends

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

Voice

- Voice is very sensitive to delays and dropped packets; there is no reason to re-transmit voice if packets are lost.
- Voice packets must receive a higher priority than other types of traffic.
- Voice can tolerate a certain amount of latency, jitter, and loss without any noticeable effects.

Video

- Compared to voice, video is less resilient to loss and has a higher volume of data per packet.
- video can tolerate a certain amount of latency, jitter, and loss without any noticeable affects.

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 is relatively insensitive to drops and delays compared to voice and video.

Prioritizing Traffic

- 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.

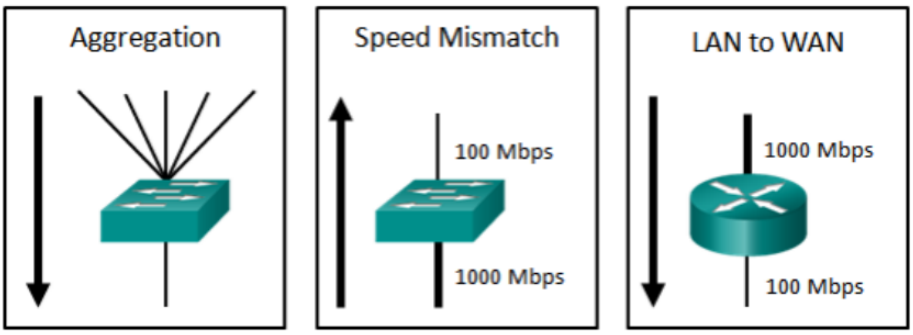
Bandwidth, Congestion, Delay, and Jitter

- Network congestion causes delay.
- Delay is the time it takes for a packet to travel from the source to the destination.
- Jitter is the variation in the delay of received packets.

Packet Loss

- When congestion occurs, network devices such as routers and switches can drop packets.
- Packet loss is a very common cause of voice quality problems on an IP network.
- In a properly designed network, packet loss should be near zero.
- Network engineers use QoS mechanisms to classify voice packets for zero packet loss.

Examples of Congestion Points



Queueing Algorithms

- First In First Out (FIFO)
  - FIFO has no concept of priority or classes of traffic and consequently, makes no decision about packet priority.
  - FIFO, which is the fastest method of queuing, is effective for large links that have little delay and minimal congestion.
- Weighted Fair Queuing (WFQ)
  - An automated scheduling method that provides fair bandwidth allocation to all network traffic.
  - Applies priority, or weights, to identified traffic and classifies it into conversations or flows.
  - WFQ is not supported with tunneling and encryption because these features modify the packet content information required

Class-Based Weighted Fair Queuing (CBWFQ)

- Extends the standard WFQ functionality to provide support for user-defined traffic classes.
- To characterize a class, you assign it bandwidth, weight, and maximum packet limit.
- You also specify the queue limit for that class, which is the maximum number of packets allowed to accumulate in the queue for the class.
- Packets belonging to a class are subject to the bandwidth and queue limits that characterize the class.

Low Latency Queuing (LLQ)

- LLQ provides strict priority queuing for CBWFQ, reducing jitter in voice conversations.
- The bandwidth assigned to the packets of a class determines the order in which packets are sent.
- Without LLQ, all packets are serviced fairly based on weight; no class of packets may be granted strict priority.
- LLQ allows delay-sensitive data such as voice to be sent first.

Selecting an Appropriate QoS Policy Model

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.

Best-Effort

Benefits	Drawbacks
The model is the most scalable.	There are no guarantees of delivery.
Scalability is only limited by bandwidth limits, 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.

Integrated services

- Uses resource reservation and admission-control mechanisms as building blocks to establish and maintain QoS.
- The edge router performs admission control to ensure that available resources are sufficient in the network.
- The IntServ standard assumes that routers along a path set and maintain the state for each individual communication.
- 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**
    - Explicit end-to-end resource admission control
    - Per-request policy admission control
    - „Hard QoS”
- **Drawbacks**
    - Resource intensive due to the stateful architecture requirement for continuous signaling.
    - Flow-based approach not scalable to large implementations such as the Internet.

Differentiated Services

- Specifies a simple and scalable mechanism for classifying and managing network traffic and providing QoS guarantees on modern IP networks.
- DiffServ can provide an “almost guaranteed” QoS while still being cost-effective and scalable.
- DiffServ uses a “soft QoS” approach. It works on the provisioned-QoS model, where network elements are set up to service multiple classes of traffic each with varying QoS requirements.
- DiffServ divides network traffic into classes based on business requirements.
- Each of the classes can then be assigned a different level of service.
- **Benefits**
    - Highly scalable
    - Provides many different levels of quality
- **Drawbacks**
    - No absolute guarantee of service quality
    - Requires a set of complex mechanisms to work in concert throughout the network

QoS tools include the following:

- **Classification and Marking**
    - Classification determines the class of traffic to which packets or frames belong. Marking means that we are adding a value to the packet header. Devices receiving the packet look at this field to see if it matches a defined policy.
- **Congestion Avoidance**
    - Congestion avoidance tools monitor network traffic loads in an effort to anticipate and avoid congestion. As queues fill up to the maximum threshold, a small percentage of packets are dropped. Once the maximum threshold is passed, all packets are dropped.
- **Shaping and Policing**
    - retains excess packets in a queue and then schedules the excess for later transmission over increments of time. Shaping is used on outbound traffic. Policing either drops or remarks excess traffic. Policing is often applied to inbound traffic.

11. Network monitoring tools, SNMP, Syslog, NTP

SNMP

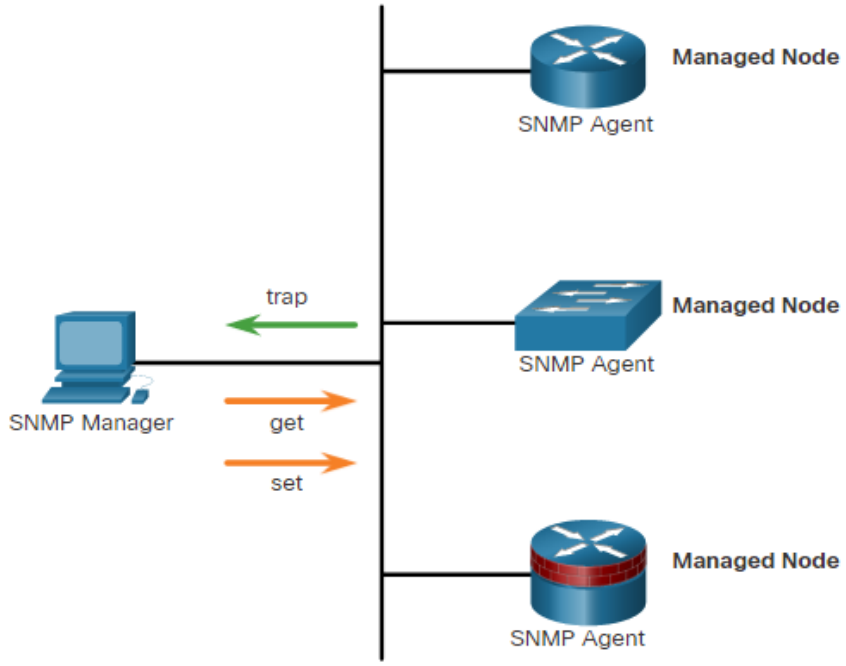
SNMP was developed to allow administrators to manage nodes such as servers, workstations, routers, switches, and security appliances, on an IP network. It enables network administrators to monitor and manage network performance, find and solve network problems, and plan for network growth.

SNMP is an application layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of three elements:

- SNMP manager
- SNMP agents (managed node)
- Management Information Base (MIB)

To configure SNMP on a networking device, it is first necessary to define the relationship between the manager and the agent.

The SNMP manager is part of a network management system (NMS). The SNMP manager runs SNMP management software. As shown in the figure, the SNMP manager can collect information from an SNMP agent by using the “get” action and can change configurations on an agent by using the “set” action. In addition, SNMP agents can forward information directly to a network manager by using “traps”.



The SNMP agent and MIB reside on SNMP client devices. Network devices that must be managed, such as switches, routers, servers, firewalls, and workstations, are equipped with an SNMP agent software module. MIBs store data about the device and operational statistics and are meant to be available to authenticated remote users. The SNMP agent is responsible for providing access to the local MIB.

SNMP defines how management information is exchanged between network management applications and management agents. The SNMP manager polls the agents and queries the MIB for SNMP agents on UDP port 161. SNMP agents send any SNMP traps to the SNMP manager on UDP port 162.

SNMP Operation

SNMP agents that reside on managed devices collect and store information about the device and its operation. This information is stored by the agent locally in the MIB. The SNMP manager then uses the SNMP agent to access information within the MIB.

There are two primary SNMP manager requests, get and set. A get request is used by the NMS to query the device for data. A set request is used by the NMS to change configuration variables in the agent device. A set request can also initiate actions within a device. For example, a set can cause a router to reboot, send a configuration file, or receive a configuration file. The SNMP manager uses the get and set actions to perform the operations described in the table.

Operation	Description
`get-request`	Retrieves a value from a specific variable.
`get-next-request`	Retrieves a value from a variable within a table; the SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
`get-bulk-request`	Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data. (Only works with SNMPv2 or later.)
`get-response`	Replies to a **get-request, get-next-request,** and **set-request** sent by an NMS.
`set-request`	Stores a value in a specific variable.

The SNMP agent responds to SNMP manager requests as follows:

Get an MIB variable - The SNMP agent performs this function in response to a GetRequest-PDU from the network manager. The agent retrieves the value of the requested MIB variable and responds to the network manager with that value.

Set an MIB variable - The SNMP agent performs this function in response to a SetRequest-PDU from the network manager. The SNMP agent changes the value of the MIB variable to the value specified by the network manager. An SNMP agent reply to a set request includes the new settings in the device.

An NMS periodically polls the SNMP agents that are residing on managed devices using the get request. The NMS queries the device for data. Using this process, a network management application can collect information to monitor traffic loads and to verify the device configurations of managed devices. The information can be displayed via a GUI on the NMS. Averages, minimums, or maximums can be calculated. The data can be graphed, or thresholds can be set to trigger a notification process when the thresholds are exceeded. For example, an NMS can monitor CPU utilization of a Cisco router. The SNMP manager samples the value periodically and presents this information in a graph for the network administrator to use in creating a baseline, creating a report, or viewing real time information.

Periodic SNMP polling does have disadvantages. First, there is a delay between the time that an event occurs and the time that it is noticed (via polling) by the NMS. Second, there is a trade-off between polling frequency and bandwidth usage.

To mitigate these disadvantages, it is possible for SNMP agents to generate and send traps to inform the NMS immediately of certain events. Traps are unsolicited messages alerting the SNMP manager to a condition or event on the network. Examples of trap conditions include, but are not limited to, improper user authentication, restarts, link status

(up or down), MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events. Trap-directed notifications reduce network and agent resources by eliminating the need for some of SNMP polling requests.

NTP

A better solution is to configure the NTP on the network. This protocol allows routers on the network to synchronize their time settings with an NTP server. A group of NTP clients that obtain time and date information from a single source have more consistent time settings. When NTP is implemented in the network, it can be set up to synchronize to a private master clock, or it can synchronize to a publicly available NTP server on the internet.

NTP networks use a hierarchical system of time sources. Each level in this hierarchical system is called a stratum. The stratum level is defined as the number of hop counts from the authoritative source. The synchronized time is distributed across the network by using NTP. The figure displays a sample NTP network.

NTP servers are arranged in three levels showing the three strata. Stratum 1 is connected to Stratum 0 clocks.

Stratum 0

An NTP network gets the time from authoritative time sources. Stratum 0 devices such as atomic and GPS clocks are the most accurate authoritative time sources. Specifically, stratum 0 devices are non-network high-precision timekeeping devices assumed to be accurate and with little or no delay associated with them. In the figure, they are represented by the clock icon.

Stratum 1

The stratum 1 devices are network devices that are directly connected to the authoritative time sources. They function as the primary network time standard to stratum 2 devices using NTP.

Stratum 2 and Lower

The stratum 2 servers are connected to stratum 1 devices through network connections. Stratum 2 devices, such as NTP clients, synchronize their time by using the NTP packets from stratum 1 servers. They could also act as servers for stratum 3 devices.

Smaller stratum numbers indicate that the server is closer to the authorized time source than larger stratum numbers. The larger the stratum number, the lower the stratum level. The max hop count is 15. Stratum 16, the lowest stratum level, indicates that a device is unsynchronized. Time servers on the same stratum level can be configured to act as a peer with other time servers on the same stratum level for backup or verification of time.

Syslog

Like a Check Engine light on your car dashboard, the components in your network can tell you if there is something wrong. The syslog protocol was designed to ensure that you can receive and understand these messages. When certain events occur on a network, networking devices have trusted mechanisms to notify the administrator with detailed system messages. These messages can be either non-critical or significant. Network administrators have a variety of options for storing, interpreting, and displaying these messages. They can also be alerted to those messages that could have the greatest impact on the network infrastructure.

The most common method of accessing system messages is to use a protocol called syslog.

Syslog is a term used to describe a standard. It is also used to describe the protocol developed for that standard. The syslog protocol was developed for UNIX systems in the 1980s but was first documented as RFC 3164 by IETF in 2001.

Syslog uses UDP port 514 to send event notification messages across IP networks to event message collectors, as shown in the figure.

Many networking devices support syslog, including: routers, switches, application servers, firewalls, and other network appliances. The syslog protocol allows networking devices to send their system messages across the network to syslog servers.

There are several different syslog server software packages for Windows and UNIX. Many of them are freeware.

The syslog logging service provides three primary functions, as follows:

- The ability to gather logging information for monitoring and troubleshooting
- The ability to select the type of logging information that is captured
- The ability to specify the destinations of captured syslog messages

Syslog Operation

On Cisco network devices, the syslog protocol starts by sending system messages and debug output to a local logging process that is internal to the device. How the logging process manages these messages and outputs is based on device configurations. For example, syslog messages may be sent across the network to an external syslog server. These messages can be retrieved without needing to access the actual device. Log messages and outputs stored on the external server can be pulled into various reports for easier reading.

Alternatively, syslog messages may be sent to an internal buffer. Messages sent to the internal buffer are only viewable through the CLI of the device.

Finally, the network administrator may specify that only certain types of system messages be sent to various destinations. For example, the device may be configured to forward all system messages to an external syslog server. However, debug-level messages are forwarded to the internal buffer and are only accessible by the administrator from the CLI.

As shown in the figure, popular destinations for syslog messages include the following:

- Logging buffer (RAM inside a router or switch)
- Console line
- Terminal line
- Syslog server

It is possible to remotely monitor system messages by viewing the logs on a syslog server, or by accessing the device through Telnet, SSH, or through the console port.

Syslog Message

Each syslog level has its own meaning:

- **Warning Level 4** - Emergency Level 0: These messages are error messages about software or hardware malfunctions; these types of messages mean that the functionality of the device is affected. The severity of the issue determines the actual syslog level applied.
- **Notification Level 5**: This notifications level is for normal, but significant events. For example, interface up or down transitions, and system restart messages are displayed at the notifications level.
- **Informational Level 6:** This is a normal information message that does not affect device functionality. For example, when a Cisco device is booting, you might see the following informational message: %LICENSE-6-EULA_ACCEPT_ALL: The Right to Use End User License Agreement is accepted.
- **Debugging Level 7:** This level indicates that the messages are output generated from issuing various debug commands.

12. WAN services, taxonomy, types and characteristics

The most commonly used WAN services and protocols

- A WAN is a telecommunications network that spans over a relatively large geographical area and is required to connect beyond the boundary of the LAN.
- WANs provide networking services over large geographical areas.
- WANs are used to interconnect remote users, networks, and sites.
- WANs are owned and managed by internet service, telephone, cable, and satellite providers.
- WAN services are provided for a fee.
- WANs providers offer low to high bandwidth speeds, over long distances.

A private WAN is a connection that is dedicated to a single customer. Private WANs provide the following:

- Guaranteed service level
- Consistent bandwidth
- Security

A public WAN connection is typically provided by an ISP or telecommunications service provider using the internet. In this case, the service levels and bandwidth may vary, and the shared connections do not guarantee security.

WANs are implemented using the following logical topology designs:

- **Point-to-Point Topology**
  - Employs a point-to-point circuit between two endpoints.
  - Involves a Layer 2 transport service through the service provider network.
  - The point-to-point connection is transparent to the customer network.
- **Hub-and-Spoke Topology**
  - Enables a single interface on the hub router to be shared by all spoke circuits.
  - Spoke routers can be interconnected through the hub router using virtual circuits and routed subinterfaces.
  - Spoke routers can only communicate with each other through the hub router.
- **Dual-homed Topology**
  - Offers enhanced network redundancy, load balancing, distributed computing and processing, and the ability to implement backup service provider connections.
  - More expensive to implement than single-homed topologies. This is because they require additional networking hardware, such as additional routers and switches.
  - More difficult to implement because they require additional, and more complex, configurations.
- **Fully Meshed Topology**
  - Uses multiple virtual circuits to connect all sites
  - The most fault-tolerant topology
- **Partially Meshed Topology**
  - Connects many but not all sites

Classification of WAN protocols

Most WAN standards focus on the physical layer and the data link layer.

Layer 1 Protocols

- Synchronous Digital Hierarchy (SDH) is a global standard for transporting data over fiber-optic cable.
- Synchronous Optical Networking (SONET) is the North American standard that provides the same services as SDH.

- Dense Wavelength Division Multiplexing (DWDM) is a newer technology that increases the data-carrying capacity of SDH and SONET by simultaneously sending multiple streams of data (multiplexing) using different wavelengths of light.

Layer 2 Protocols

- Broadband (i.e., DSL and Cable)
- Wireless
- Ethernet WAN (Metro Ethernet)
- Multiprotocol Label Switching (MPLS)
- Point-to-Point Protocol (PPP) (less used)
- High-Level Data Link Control (HDLC) (less used)
- Frame Relay (legacy)
- Asynchronous Transfer Mode (ATM) (legacy)

Circuit-switched networks

- A circuit-switched network establishes a dedicated circuit (or channel) between endpoints before the users can communicate.
- Establishes a dedicated virtual connection through the service provider network before communication can start.
- All communication uses the same path.
- The two most common types of circuit switched WAN technologies are the public switched telephone network (PSTN) and the legacy Integrated Services Digital Network (ISDN).

Packet-Switched networks

- Network communication is most commonly implemented using packet-switched communication.
- Segments traffic data into packets that are routed over a shared network.
- Much less expensive and more flexible than circuit switching.
- Common types of packet-switched WAN technologies are:
    - Ethernet WAN (Metro Ethernet),
    - Multiprotocol Label Switching (MPLS)
    - Frame Relay
    - Asynchronous Transfer Mode (ATM).

13. The goal, operation, and classification of different types of attacks and the main Components of the defense

Goals

- **Theft of intellectual property** means violation of intellectual property rights like copyrights, patents etc.
- **Identity theft** means to act someone else to obtain person's personal information or to access vital information they have like accessing the computer or social media account of a person by login into the account by using their login credentials.
- **Theft of equipment and information** is increasing these days due to the mobile nature of devices and increasing information capacity.
- **Sabotage** means destroying company's website to cause loss of confidence on part of its customer.
- **Information extortion** means theft of company's property or information to receive payment in exchange. For example ransomware may lock victims file making them inaccessible thus forcing victim to make payment in exchange. Only after payment victim's files will be unlocked.

Threats

- **Computer Viruses**: Perhaps the most well-known computer security threat, a computer virus is a program written to alter the way a computer operates, without the permission or knowledge of the user. A virus replicates and executes itself, usually doing damage to your computer in the process.
    - Viruses can replicate themselves by hooking them to the program on the host computer like songs, videos etc. and then they travel all over the Internet.
    - Worms are also self-replicating in nature but they don't hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network aware. They can easily travel from one computer to another if network is available on the target machine
    - The Concept of Trojan is completely different from the viruses and worms. Their purpose is to conceal themselves inside the software that seem legitimate and when that software is executed they will do their task of either stealing information or any other purpose for which they are designed. They often provide backdoor gateway for malicious programs or malevolent users to enter your system and steal your valuable data without your knowledge and permission.
    - Bots can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need of human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called Botnet.
- **Spyware Threats**: A serious computer security threat, spyware is any program that monitors your online activities or installs programs without your consent for profit or to capture personal information.
- **Hackers and Predators**: People, not computers, create computer security threats and malware. Hackers and predators are programmers who victimize others for their own gain by breaking into computer systems to steal, change, or destroy information as a form of cyber-terrorism. These online predators can compromise credit card information, lock you out of your data, and steal your identity.
- **Phishing**: Acting as a trustworthy person or business, phishers attempt to steal sensitive financial or personal information through fraudulent emails, messages or websites. Phishing attacks are some of the most successful methods for cybercriminals looking to pull off a data breach.

Reconnaissance Attacks

- Knowledge gathering attacks
- Packet sniffing, phishing, social engineering, internet information queries

Access Attacks

- Intrusion attacks
- Gaining credentials, brute forcing, plugging foreign device into the network, social engineering

Denial of Service Attacks (DDOS)

- Flooding the network with junk traffic
- Renders the network inoperable

Network Security Layers

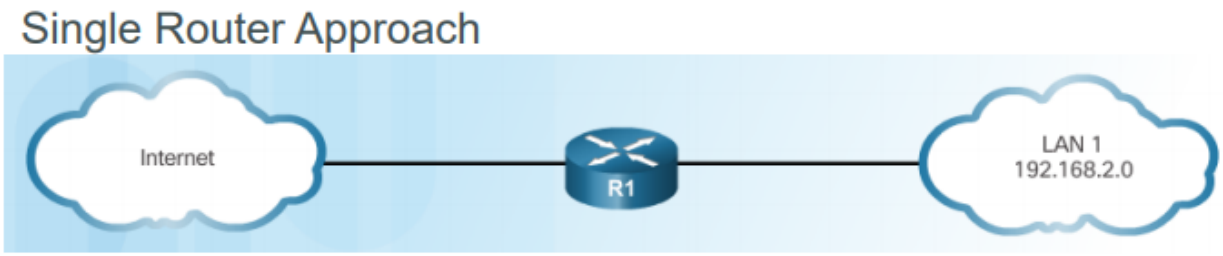
- **Physical Network Security**: Physical security controls are designed to prevent unauthorized personnel from gaining physical access to network components such as routers, cabling cupboards and so on. Controlled access, such as locks, biometric authentication and other devices, is essential in any organization.
- **Technical Network Security**: Technical security controls protect data that is stored on the network or which is in transit across, into or out of the network. Protection is twofold; it needs to protect data and systems from unauthorized personnel, and it also needs to protect against malicious activities from employees.
- **Administrative Network Security**: Administrative security controls consist of security policies and processes that control user behavior, including how users are authenticated, their level of access and also how IT staff members implement changes to the infrastructure.

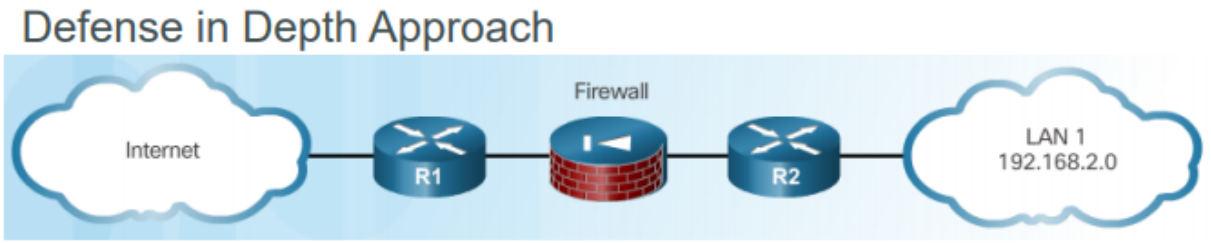
Network Security Tools

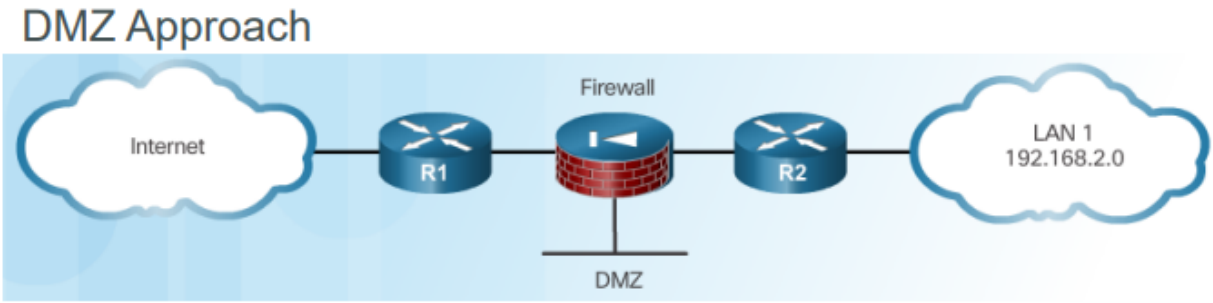
- **Network Access Control:** To ensure that potential attackers cannot infiltrate your network, comprehensive access control policies need to be in place for both users and devices. Network access control (NAC) can be set at the most granular level. For example, you could grant administrators full access to the network but deny access to specific confidential folders or prevent their personal devices from joining the network.
- **Antivirus and Antimalware Software:** Antivirus and antimalware software protect an organization from a range of malicious software, including viruses, ransomware, worms and trojans. The best software not only scans files upon entry to the network but continuously scans and tracks files.
- **Firewall Protection:** Firewalls, as their name suggests, act as a barrier between the untrusted external networks and your trusted internal network. Administrators typically configure a set of defined rules that blocks or permits traffic onto the network.
- **Virtual Private Networks:** Virtual private networks (VPNs) create a connection to the network from another endpoint or site. For example, users working from home would typically connect to the organization's network over a VPN. Data between the two points is encrypted and the user would need to authenticate to allow communication between their device and the network.

14. The defense of networking devices, edge devices, purpose and advantages, disadvantages of centralized protection

Edge Router Security Approaches







Three areas of router security

Physical Security

- Place the router and physical devices that connect to it in a secure locked room that is accessible only to authorized personnel, is free of electrostatic or magnetic interference, has fire suppression, and has temperature and humidity controls.
- Install an uninterruptible power supply (UPS) or diesel backup power generator, and keep spare components available.

Operating system and configuration file security

- Configure the router with the maximum amount of memory possible.
- Use the latest, stable version of the operating system that meets the feature specifications of the router or network device.
- Keep a secure copy of router operating system images and router configuration files as backups.

Router Hardening

- Secure administrative control.

- Disable unused ports and interfaces. Disable unnecessary services.

Secure Administrative Access

- Restrict device accessibility
- Log and account for all access
- Authenticate access
- Authorize actions
- Present legal notification
- Ensure the confidentiality of data

Authentication without AAA

Configure a login and password combination on console, vty lines, and aux ports

- Easy to implement
- Weak and least secure
- Anyone with the password can enter

Telnet, SSh

- More secure, username and password is needed
- Has to be configured locally on each device, no fallback authentication method

AAA

- A better solution is to have all devices refer to the same database of usernames and passwords from a central server.
- who is permitted to access a network (authenticate)
- what they can do while they are there (authorize)
- and to audit what actions they performed while accessing the network (accounting).

AAA Components

Authentication

- Authentication can be established using username and password combinations, challenge and response questions, token cards, and other methods.

Authorization

- Authorization services determine which resources the user can access and which operations the user is allowed to perform.

Accounting

- Records what the user does, including what is accessed, the amount of time the resource is accessed, and any changes that were made.

Authentication

Local AAA Authentication

- stores usernames and passwords locally in the Cisco router, and users authenticate against the local database
- ideal for small networks

Server-based AAA Authentication

- The central AAA server contains the usernames and password for all users
- When there are multiple routers and switches, server-based AAA is more appropriate

Authorization

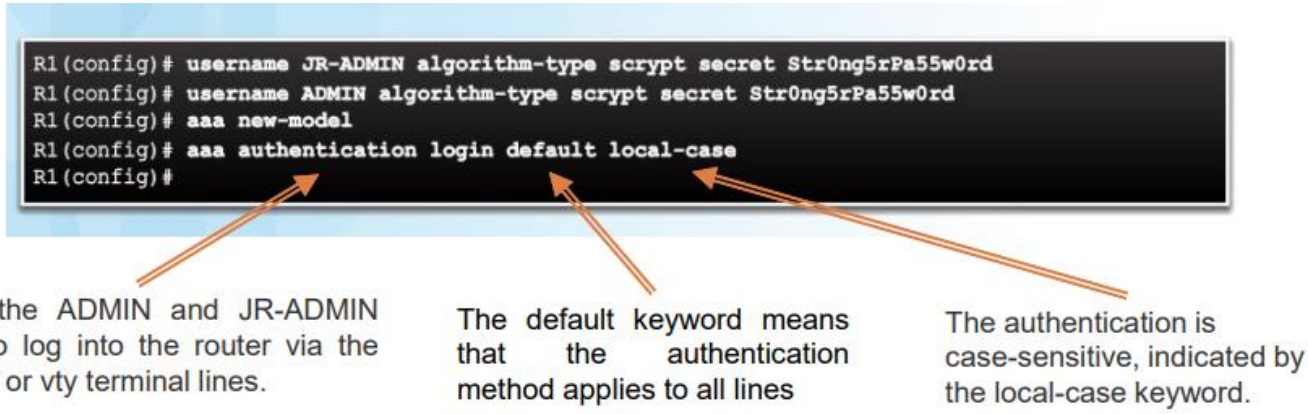
1. When a user has been authenticated, a session is established between the router and the AAA server.
2. The router requests authorization from the AAA server for the client's requested service.
3. The AAA server returns a PASS/FAIL for authorization.

Authorization is automatic and does not require users to perform additional steps after authentication. Authorization is implemented immediately after the user is authenticated.

Accounting

1. When a user has been authenticated, the AAA accounting process generates a start message to begin the accounting process.
2. When the user finishes, a stop message is recorded and the accounting process ends.

AAA Accounting collects and reports usage data. The collected data might include the start and stop connection times, executed commands, number of packets, and number of bytes. The log contains numerous data fields, including the username, the date and time, and the actual command that was entered by the user. This information is useful when troubleshooting devices.




```
Router(config)#
aaa local authentication attempts max-fail [number-of-unsuccessful-attempts]
```

This command secures AAA user accounts by locking out accounts that have excessive failed attempts.

	TACACS+	RADIUS
Functionality	Separates AAA according to the AAA architecture, allowing modularity of the security server implementation	Combines authentication and authorization but separates accounting, allowing less flexibility in implementation than TACACS+
Standard	Mostly Cisco supported	Open/RFC standard
Transport Protocol	TCP	UDP
CHAP	Bidirectional challenge and response as used in Challenge Handshake Authentication Protocol (CHAP)	Unidirectional challenge and response from the RADIUS security server to the RADIUS client
Confidentiality	Entire packet encrypted	Password encrypted
Customization	Provides authorization of router commands on a per-user or per-group basis	Has no option to authorize router commands on a per-user or per-group basis
Accounting	Limited	Extensive

Configuring Server-Based AAA Authentication

1. Globally enable AAA to allow the use of all AAA elements. This step is a prerequisite for all other AAA commands.
    - Enable AAA
2. Specify the SERVER that will provide AAA services for the router. This can be a TACACS+ or RADIUS server.
    - Specify the IP address of the server
3. Configure the encryption key needed to encrypt the data transfer between the network access server.
    - Configure the secret key
4. Configure the AAA authentication method list to refer to the TACACS+ or RADIUS server. For redundancy, it is possible to configure more than one server.
    - Configure authentication to use either the RADIUS or TACACS+ server

When AAA authorization is not enabled, all users are allowed full access.

After authentication is started, the default changes to allow no access.

The administrator must create a user with full access rights before authorization is enabled

Advantages of centralized:

- Flexible, scalable
- Better security
- Central point for user management

Disadvantages of centralized:

- Maintanance, on-prem management
- Initial setup
- Many options

802.1x

IEEE 802.1X is a standard that defines how to provide authentication for devices that connect with other devices on local area networks (LANs).

It provides a mechanism by which network switches and access points can hand off authentication duties to a specialized authentication server, like a RADIUS server, so that device authentication on a network can be managed and updated centrally, rather than distributed across multiple pieces of networking hardware.

15. The concept, condition and implementation possibilities of traffic filtering with IPv4 and IPv6

Purpose of ACLs: Packet Filtering

- Packet filtering, sometimes called static packet filtering, controls access to a network by analyzing the incoming and outgoing packets and passing or dropping them based on given criteria, such as the source IP address, destination IP addresses, and the protocol carried within the packet.
- A router acts as a packet filter when it forwards or denies packets according to filtering rules.
- An ACL is a sequential list of permit or deny statements, known as access control entries (ACEs).

An inbound ACL filters packets coming into a specific interface and before they are routed to the outbound interface.

An outbound ACL filters packets after being routed, regardless of the inbound interface.

The last statement of an ACL is always an implicit deny. This statement is automatically inserted at the end of each ACL even though it is not physically present. The implicit deny blocks all traffic. Because of this implicit deny, an ACL that does not have at least one permit statement will block all traffic.

Standard ACLs

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

Standard ACLs filter IP packets based on the source address only.

Extended ACLs

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

Extended ACLs filter IP packets based on several attributes, including the following:

- Source and destination IP addresses
- Source and destination TCP and UDP ports
- Protocol type/ Protocol number (example: IP, ICP, UDP, TCP, etc.)

Numbered ACL:

You assign a number based on which protocol you want filtered:
- (1 to 99) and (1300 and 1999): Standard IP ACL
- (100 to 199) and (2000 to 2699): Extended IP ACL

Named ACL:

You assign a name by providing the name of the ACL:
- Names can contain alphanumeric characters.
- It is suggested that the name be written in CAPITAL LETTERS.
- Names cannot contain spaces or punctuation.
- You can add or delete entries within the ACL.

Guidelines for creating ACLs

- **One ACL per protocol** - To control traffic flow on an interface, an ACL must be defined for each protocol enabled on the interface.
- **One ACL per direction** - ACLs control traffic in one direction at a time on an interface. Two separate ACLs must be created to control inbound and outbound traffic.
- **One ACL per interface** - ACLs control traffic for an interface, for example, GigabitEthernet 0/0.

Placement

Every ACL should be placed where it has the greatest impact on efficiency. The basic rules are:

- Extended ACLs - Locate extended ACLs as close as possible to the source of the traffic to be filtered.
- Standard ACLs - Because standard ACLs do not specify destination addresses, place them as close to the destination as possible.

Placement of the ACL and therefore the type of ACL used may also depend on: the extent of the network administrator's control, bandwidth of the networks involved, and ease of configuration.

Standard ACL to Secure VTY

Filtering Telnet or SSH traffic is typically considered an extended IP ACL function because it filters a higher level protocol. However, because the access-class command is used to filter incoming or outgoing Telnet/SSH sessions by source address, a standard ACL can be used.

Configuring Extended ACLs

The procedural steps for configuring extended ACLs are the same as for standard ACLs. The extended ACL is first configured, and then it is activated on an interface. However, the command syntax and parameters are more complex to support the additional features provided by extended ACLs.

Inbound ACL logic

- Packets are tested against an inbound ACL, if one exists, before being routed.
- If an inbound packet matches an ACL statement with a permit, it is sent to be routed.
- If an inbound packet matches an ACL statement with a deny, it is dropped and not routed.
- If an inbound packet does not meet any ACL statements, then it is "implicitly denied" and dropped without being routed.

Outbound ACL logic

- Packets are first checked for a route before being sent to an outbound interface. If there is no route, the packets are dropped.
- If an outbound interface has no ACL, then the packets are sent directly to that interface.
- If there is an ACL on the outbound interface, it is tested before being sent to that interface.
- If an outbound packet matches an ACL statement with a permit, it is sent to the interface.
- If an outbound packet matches an ACL statement with a deny, it is dropped.
- If an outbound packet does not meet any ACL statements, then it is "implicitly denied" and dropped.

ACL operation

- When a packet arrives at a router interface, the router process is the same, whether ACLs are used or not. As a frame enters an interface, the router checks to see whether the destination Layer 2 address matches its the interface Layer 2 address or if the frame is a broadcast frame.
- If the frame address is accepted, the frame information is stripped off and the router checks for an ACL on the inbound interface. If an ACL exists, the packet is tested against the statements in the list.
- If the packet is accepted, it is then checked against routing table entries to determine the destination interface. If a routing table entry exists for the destination, the packet is then switched to the outgoing interface, otherwise the packet is dropped.
- Next, the router checks whether the outgoing interface has an ACL. If an ACL exists, the packet is tested against the statements in the list.
- If there is no ACL or the packet is permitted, the packet is encapsulated in the new Layer 2 protocol and forwarded out the interface to the next device.

Standard ACL process

- Standard ACLs only examine the source IPv4 address. The destination of the packet and the ports involved are not considered.
- Cisco IOS software tests addresses against the conditions in the ACL. The first match determines whether the software accepts or rejects the address. Because the software stops testing conditions after the first match, the order of the conditions is critical. If no conditions match, the address is rejected.

Extended ACL process

- The ACL first filters on the source address, then on the port and protocol of the source. It then filters on the destination address, then on the port and protocol of the destination, and makes a final permit or deny decision.

IPv6 ACLs

- Named only
- Similar in functionality to IPv4 Extended ACL

Although IPv4 and IPv6 ACLs are very similar, there are three significant differences between them.

- **Applying an IPv6 ACL** IPv6 uses the ipv6 traffic-filter command to perform the same function for IPv6 interfaces.
- **No Wildcard Masks** The prefix-length is used to indicate how much of an IPv6 source or destination address should be matched.
- **Additional Default Statements**
    - permit icmp any any nd-na: Allows ICMP neighbor discovery acknowledgements.
    - permit icmp any any nd-ns: Allows ICMP neighbor discovery solicitations.

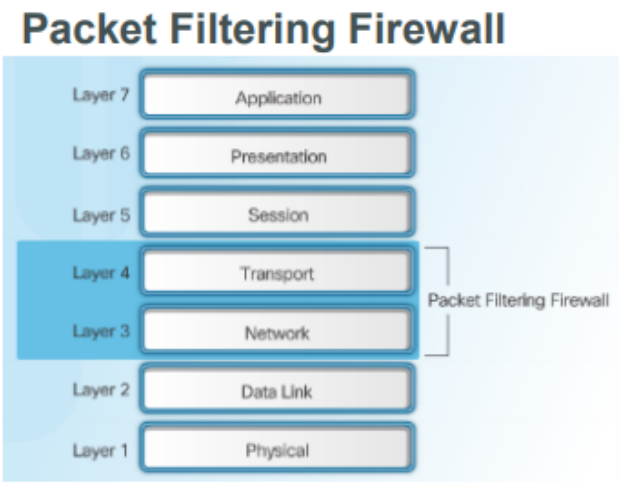
16. Firewall generations, types, architectures, firewall implementations on ISR routers, dedicated firewalls

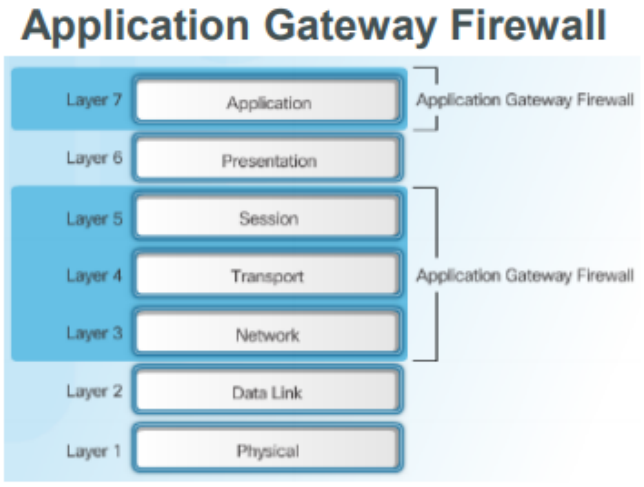
Firewall characteristics

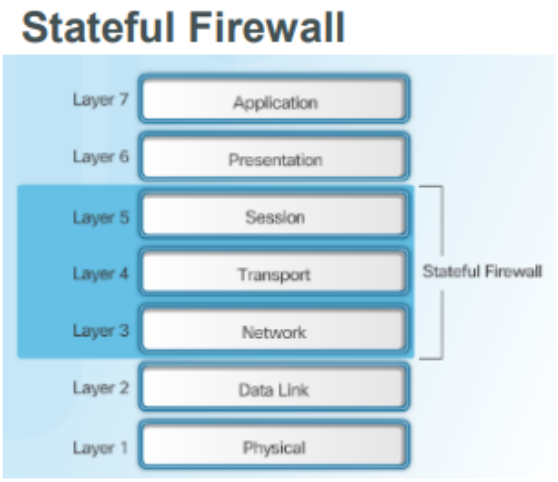
- All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
- Even with a firewall, there are still many areas of risk for your network. The most obvious is malware. -> other security tools should be used
- Disadvantages: costs, cumbersome to prepare and it also enforce annoying limitations to internal users as well

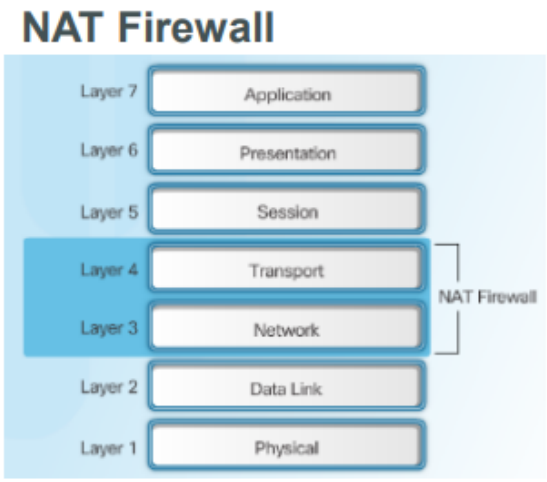
Firewalls do no provide

- Useless against attacks from the inside
- Protect against insiders/ connections that do not go through it. (wireless)
- Useless against zero-day attacks
- Firewalls should be updated from time to time
- Cannot protect against transfer of all virus infected programs or files
- Antimalware protection for encrypted traffic is difficult or impossible









1st generation: Packet filtering firewall

- It works at layer 3 and 4 (OSI)
- Decisions are based on
    - Source / destination MAC address
    - Source / destination IP address
    - Encapsulated protocol into the IP packet (TCP, UDP, ICMP, ...)
    - Source / destination port address
- The information provided in the packet header is compared to the firewall rules in a predefined order!
- If packet matches one of the rules, than the action is carried out based on the rule
- If not than there is a default action(implicit deny) White List vs. black List…
- Does not handles connection states
- Provides low level security
- Complex configuration
- Duplex traffic should be handled with two rulesets applied in the different directions
- There are some protocols that negotiates port numbers dynamically (FTP) in that cases port ranges should be enabled

2nd generation: Stateful firewall

- Stateless packet filtering:
    - ACLs filter traffic based on source and destination IP addresses, TCP and UDP port numbers, TCP flags, and ICMP types and codes.
- Stateful packet filtering:
    - Inspection remembers certain details, or the state of that request.
    - Device maintains records of all connections passing through the firewall, and is able to determine whether a packet is the start of a new connection, or part of an existing connection.
    - A stateful firewall monitors the state of connections, whether the connection is in an initiation, data transfer, or termination state.
- Note:
    - A packet-filtering firewall typically can filter up to the transport layer, while a stateful firewall can filter up to the session layer.

Benefits	Limitations
Primary means of defense	No Application Layer inspection
Strong packet filtering	Cannot filter stateless protocols
Improved performance over packet filters	Difficult to defend against dynamic port negotiation
Defends against spoofing and DoS attacks	No authentication support
Richer data log	

Next generation firewalls

- Granular identification, visibility, and control of behaviors within applications
- Restricting web and web application use based on the reputation of the site
- Proactive protection against Internet threats
- Enforcement of policies based on the user, device, role, application type, and threat profile

- Use of an IPS (Intrusion Prevention System)

Application level firewall

- Two subcategories:
  - Proxy Firewalls
  - Deep Packet Inspection Firewalls
- Operate at the 7th layer of the OSI model.
- Advantages:
  - High level security
  - Easier to configure than packet filter firewalls
- Disadvantages:
  - High CPU load
  - Vendors should follow new protocols
  - No transparency (with proxy)

Proxy firewalls

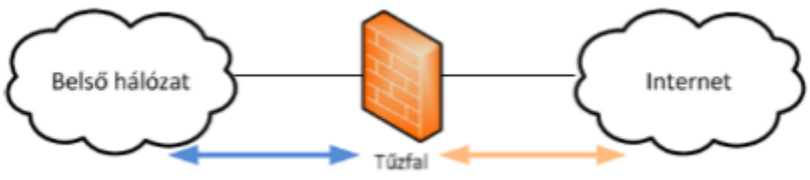
- It runs Proxy applications, that create separate connections with the two communicating parties.
- The indirect connections breaks, the proxy gateway recreates the packets that should be forwarded, with copying the required protocol fields.
- A proxy server represents the network from the outside. Any user trying to gain access to any computer inside a network with a proxy will only see the IP address of the proxy server. It acts like a barrier to hide your network by configuring the Internet options of computers within the network to first point to the proxy server before going out to the Internet. It keeps computers inside the network anonymous.
- „Packets are coming from an infected client is recreated without bullshit”
- For every application type a separate proxy server is needed. HTTP proxy recreates only HTTP traffic fields.

Deep packet inspection firewalls

- It works transparently, does not set up connections with the two communicating parties.
- Filters in all 7 layers of the OSI model
- Filters the packets that are not appropriate according the protocol.
- Categorizes the packets according to different applications

Dual-homed

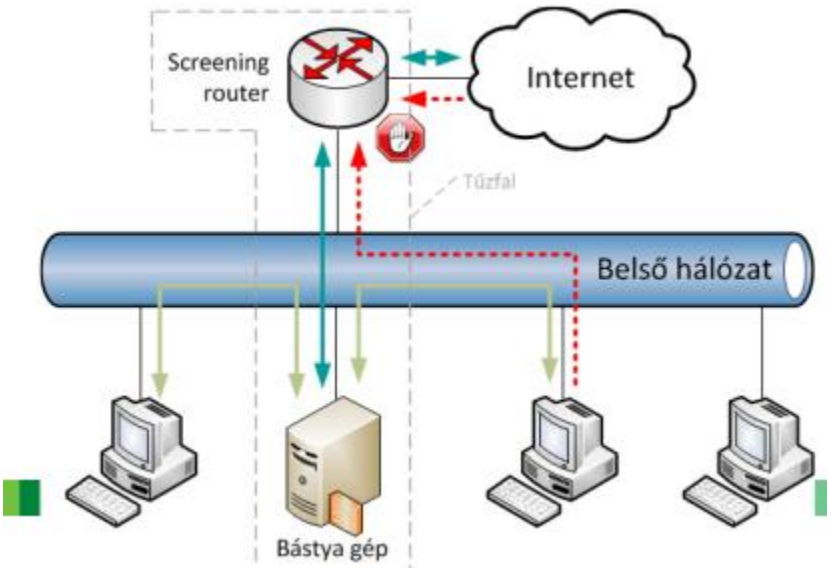
- It has two network connections, connecting to different networks and performing filtering between them
- It can be SPI, DPI, Proxy, stb…
- Two Leg Perimeter
- Special case: – router is a firewall: screening router



Single-homed

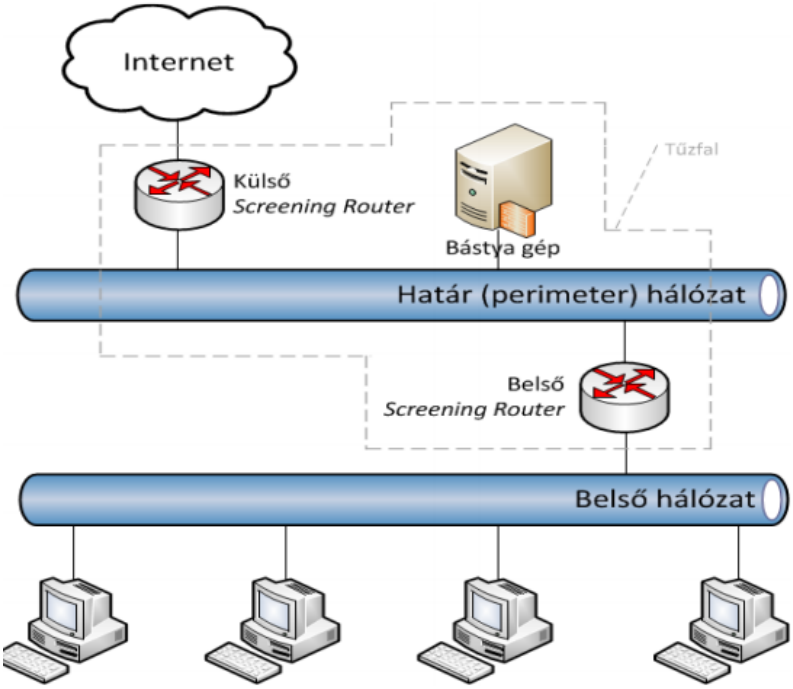
- This architectures provides services that the service provider bastion host has only one interface attached to the internal network.

- The primary defense is provided by a packet filter router (screening router), it prevents user devices to indirectly access internet.
- Internet hosts can connect to only the bastion host.
- The security of the bastion host is very important
- The bastion host works as a proxy
- A screening router can be configured that some services are accessible indirectly and others are only accessible through the proxy



Disadvantage:

- If an attacker gains access to the bastion host, nothing prevents him/her to enter the intranet.
- screened subnet architecture is more reliable
- screened-subnet architecture places one more security layer between the intranet and the internet. -> perimeter network



Perimeter network:

- If an attacker gains access to the bastion host, it only affects the traffic of the perimeter network, not the intranet traffic.
- Every traffic destined to the internet and to the bastion host goes through the perimeter network, but traffic between two internal host does not go through the perimeter network.

Bastion host:

- It handles the incoming traffic (SMTP, FTP, DNS WWW, …)
- Traffic going outward can be handled in two different way:
    - With packet filter rules taking place on the inner and outer screening routers
    - With proxy servers on the bastion host.

Internal router (Choke router):

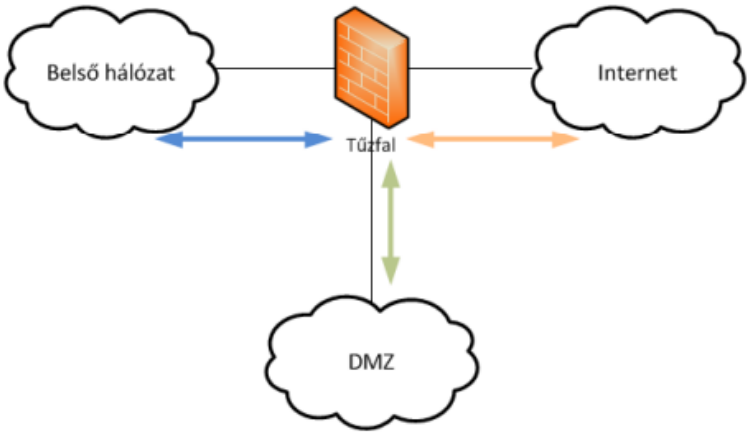
- It controls which services can be accessed from the inside network indirectly. (Telnet, Fttp, Http,)
- It controls the traffic between the inside network and the bastion host. The number of these kind of services should be decreases that the attack surface of the inner network should be minimized.

External router (Access router):

- Protects the perimeter and the inner network from the internet.
- It usually enables all traffic going out.
- Packet filter rules (protecting the inner network) on both screening routers are the same.

Multi-homed

- The firewall has 3 or more network interfaces and filters traffic between them.
- The firewall can be SPI, DPI, Proxy, …
- Three Leg Perimeter



Demilitarized Zone

- Perimeter network.
- Network segment that provides services to the untrusted network (internet).
- Usually it has a security level that is different from the internal and the external network. It's purpose to provide an extra layer of security in a way, that external attacker cannot access the trusted internal network, just through a firewall.
- The trusted intranet can also use the services provided by the DMZ.

CBAC – Context-Based Access Control

- Stateful packet filtering at layer 3,4,5
- Traffic inspection
- Intrusion detection
- Filters only the configured traffic, based on access lists

- Stores information about TCP, UDP and ICMP connection in the state table
- It creates dynamic entries for filtering incoming traffic
- Creates temporary openings for established sessions and connections, typically to allow reply packets
- When the application terminates removes the corresponding dynamic ACLs

Zone-Based Policy Firewall

- Interfaces are assigned to zones
- Inspection policy is applied to traffic moving between them
- Default is to deny all traffic
- Advantages
    - Easy to use, well structured
    - Not dependent on ACLs
    - Policies are easy to read and troubleshoot
    - One policy affects any given traffic, instead of needing multiple ACLs
- Subnetworks residing in the same zone can communicate with each other
- More than one interface can be in one zone, but one interface can only be in one zone
- Inspect: allows for return traffic and ICMP
- Pass: permit statement, allowing traffic in one direction
- Drop: deny statement, can be logged
- The router itself is not part of the zones, but has its own Self Zone, for which policies can be applied

1. Create Zones
2. Identify traffic with class maps
3. Define actions with policy maps
4. Identify zone pairs and match to policy
5. Assign zones to interfaces

ASA is a dedicated firewall device

- high encryption capability
- Filtering large volume traffic
- Big amount VPN termination

Extra features

- botnetfilter
- threat detection
- application inspection

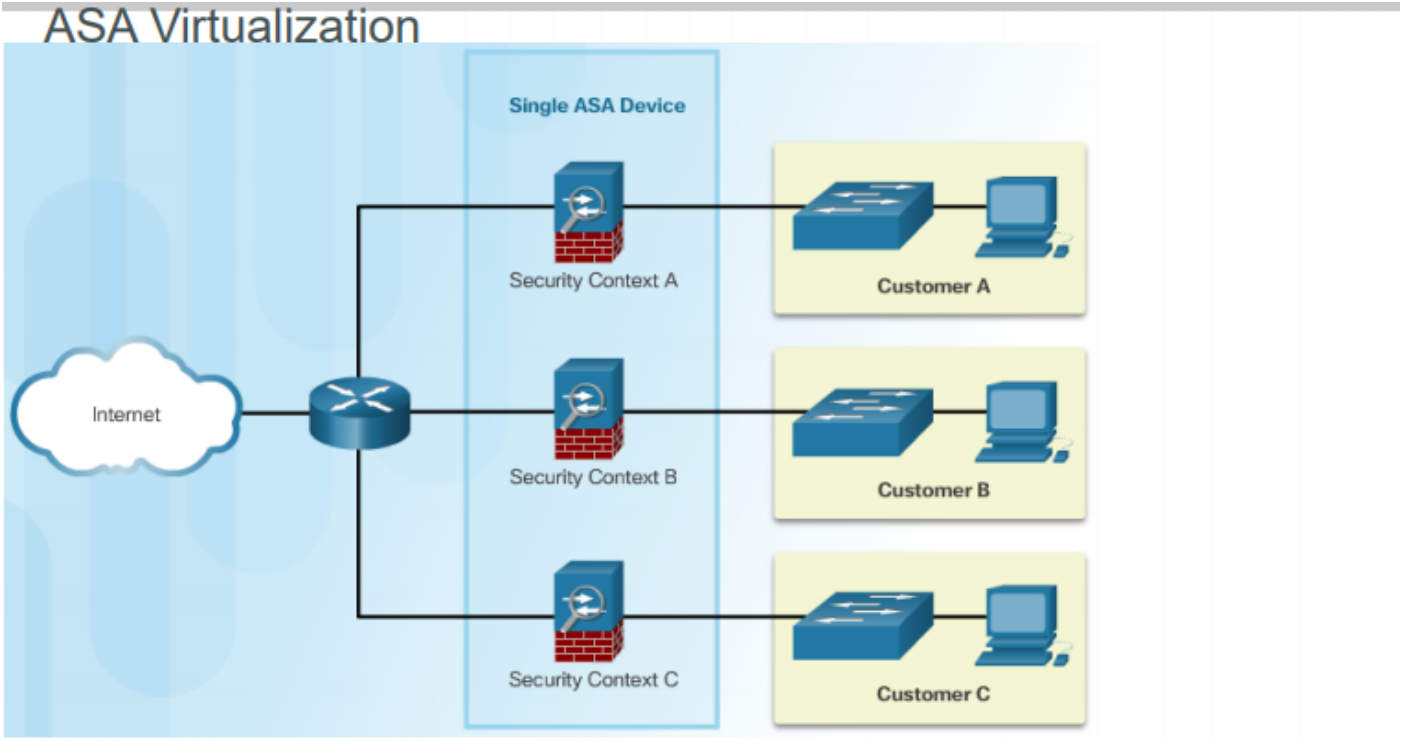
Basics

- Packetfiltering mechanism
- Stateful operation
- Transparent or Routed mode
- Multi-context
- IPS or NGFW

Fields of application

- Edge protection
- Protection against external attacks
- Address translation
- VPN termination
- Separating different segments of networks

- Mainly firewall operation, the segments can iniate limited communication with each other



A single ASA can be partitioned into multiple virtual devices, as illustrated in Figure (context).
Many features are supported in multiple context modes, including routing tables, firewall features, IPS, and management.

ASA Failover

High Availability
Redundancy
For failover we apply ASA devices in pairs which are of:

- same type
- Same hardware structure
- Having the right license
- Active/active: both ASA devices transmit traffic
- Active/standby: only one is forwarding
- Stateful/stateless
- Dedicated connection between them with
    - Failover cable
    - Dedicated LAN interface: with a switch or directly
- Active/standby failover
    - Only one device forwards traffic
    - It can be used in one or multicontext scenario
    - (context = One physical device can be separated into more virtual firewalls. One virtual firewall is a context)

Data sent through the failover link

- **Stateless** (regular): during change the connections are lost

    - State (active or standby)
    - Hello messages (keep-alive)
    - Link state
    - configuration synchronization
- **Stateful**: additional information for preventing connection loss
    - NAT table
    - TCP connection state
    - UDP connection state
    - ARP table
    - L2 bridge table (transparent mode)
    - HTTP connection state
    - ISAKMP and IPSec SA table

ASA Modes of operation

- **Transparent**
    - Acts as a layer 2 device
    - Transporting non-IP traffic
    - Does not support VPN termination (only for management traffic), routing, QoS, DHCP relay
- **Routed**
    - Acts as a router
    - One (sub)interface is one subnet
    - supports dynamic routing protocols,
    - VPN termination

ASA Stateful

- It mantains a table about the actual connections (distinguishes the connections based on IP address and ports)
- SYN packet -> new connection
- Packets belonging to an already existing connections should not be investigated in a so detailed manner
- Answer for inside
    - outside traffic can go through the ASA without incoming ACL permission, beacuse it belongs to already ESTABLISHED connection

Security level

- Assigned to the Interfaces (physical or logical)
- number between 0-100, representing the reliability (the higher the better)
- For example Inside 100, DMZ 50, Outside 0

Configuration

- From global configuration mode: ASA host name, domain name, and privileged EXEC mode password
- At first Switch Virtual Interfaces (SVIs) should be configured, we assign the names, security level, and IP address
- Layer 2 ports are assigned to SVI VLANs
- By default all ports are in VLAN 1
- inside and outside SVI-s can be configured
- ip addresses
- static routes
- telnet, ssh
- dhcp services

ASA ACLs

- ASA ACL uses subnet mask (e.g., 255.255.255.0).
    - IOS ACL uses wildcard mask (e.g., 0.0.0.255).
- No numbered ACLs .
    - ASA ACLs are named ACLs but the name can be a number as well.
- By default the security levels also realize some filtering mechanism.
- Supports 5 types: Extended, Standard, Ipv6, Webtype, Ethertype

Usage of ACLs

- Through-traffic packet filtering:
    - To filter traffic coming from one interface of the ASA to another.
    - ACL- must be configured and applied on an interface
- To-the-box-traffic packet filtering (management access rule):
    - Telnet, SSH, SNMP traffic to the device.

ASA NAT

- Like IOS routers, the ASA supports the following NAT and PAT deployment methods:
- **Inside NAT**
    - Typical NAT deployment method when the ASA translates the internal host address to a global address.
    - The ASA restores return traffic the original inside IP address.
- **Outside NAT**
    - Deployment method used when traffic from a lower-security interface is destined for a higher-security interface.
    - This method may be useful to make a host on the outside appear as one from a known internal IP address.
- **Bidirectional NAT**
    - Both inside NAT and outside NAT are used together. ASA NAT Services
- **Dynamic NAT**
    - Many-to-many translation.
    - Typically deployed using inside NAT.
- **Dynamic PAT**
    - Many-to-one translation.
    - Usually an inside pool of private addresses overloading an outside interface or outside address.
    - Typically deployed using inside NAT.
- **Static NAT**
    - A one-to-one translation.
    - Usually an outside address mapping to an internal server.
    - Typically deployed using outside NAT.

17. The different cryptographic tools serving authentication, integrity and confidentiality

Authentication

- Deals with Origin Authentication
    - Guarantees that message is not forgery and actually comes from whom it states
    - Typically ensured with protocols, such as hash message authentication code (HMAC)
- HMAC (Hash Message Authentication Code)
    - It is calculated by an algorithm combining a hash function and a secret key
    - Only the sender and receiver know the secret key
    - Output of the hasing data depends on both the input data and the secret key
    - It can only be digested with the secret key, eliminating man in the middle attacks and providing authentication of the sender
    - The sender device inputs data (e.g. plaintext and the secret key) and calculates an HMAC digest, which is attached to the message
    - The receiver uses the same plaintext and secret key to calculate the HMAC digest themselves, and if its equal to the one attached to the message, it was unaltered, and the origin is authenticated

Hashing functions

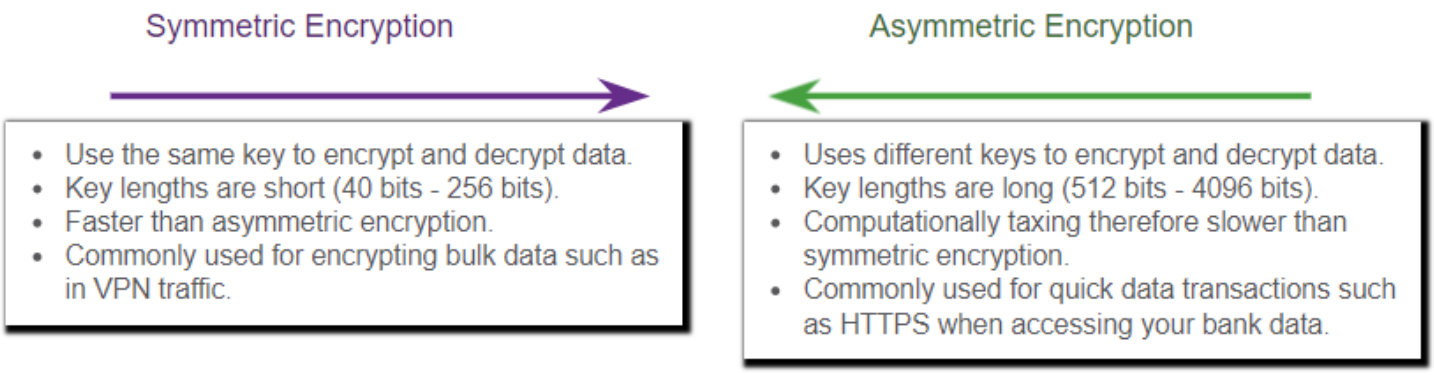
- Deal with Data Integrity
    - Guarantees that messages were not altered, any change to data during transfer will be detected
    - Ensured with hashing algorithms such as MD5 or SHA
- Hash functions
    - The sender computes a hash based on the input and attaches it to the message
    - The receiver computes a hash with the same algorithm, and if their own and the attached hash is equal, the message has not been altered
- MD5
    - One-way, legacy algorithm, produces a 128-bit hash, shouldn't be used
- SHA-1
    - Very similar to MD5 but slower, multiple versions exist, produces a 160-bit hash, legacy and shouldn't be used
- SHA-2
    - Includes 224, 256, 384 and 512 bit versions, should be used whenever possible
- Hashing only protects against accidental changes, because there is no unique identyfing information from the sender
- With the right hash functions, anyone can change the message, calculate the right hash, and attach it to the message

Vulnerable to man-in-the-middle attacks

Encryption

- Ensures Data Confidentiality
    - Only authorized users can read the message
    - If the message is interceted, it cannot be deciphered in a reasonable amount of time
- Two types of encryption algorithms, symmetric and asymmetric
    - They differ in how they use keys

- Symmetric encryption algorithms like DES or AES are based on the premise that both communication parties know the pre-shared key
- Asymmetric encryption algorithms like RSA or PKI use different keys



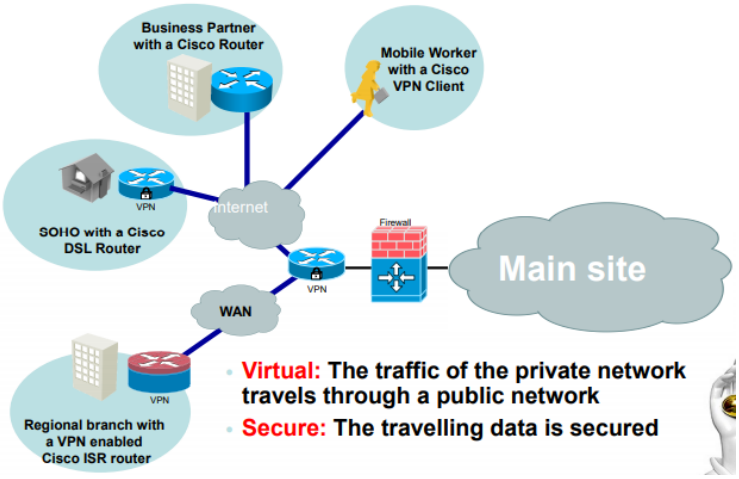
- Symmetric Encryption
  - use a pre-shared key to encrypt and decrypt data
  - pre-shared key, or secret key is known by both sender and receiver before communication
  - commonly used with VPN traffic
  - they use less CPU resources then asymmetric, which makes the process fast
  - DES is a legacy symmetric encryption algorithm, usually operating in block mode, encrypting data in 64 bit blocks. 3DES usues three independent keys per block, and is significantly stronger
  - AES is secure and more efficient, popular and recommended and works with variable key lengths
- Asymmetric Encryption
  - The key used for encryption is different than the one used for decryption
  - They cannot be calculated from each other in a reasonable time
  - They use a private key and a public key
  - Data encrypted with the public key requires the private key to decript, and vica versa
  - Because there is no shared key, very long keys are used
  - IKE, SSL, SSH use asymmetric encryption
  - Substentially slower than symmetric algorithms
  - Typically used for digital signatures and key exchange
  - Diffie-Hellman algorithm allows two parties to agree on a key that they can use for encryption
    - Two computers generate an identical shared secret key without any prior communication
    - The new shared key is never actually exchanged between them, but both parties know it, so they can use it to encrypt traffic
    - Has different groups based on the key sizes
  - RSA encryption algorithm
    - RSA is for public-key cryptography, suitable for sigining and ecryption

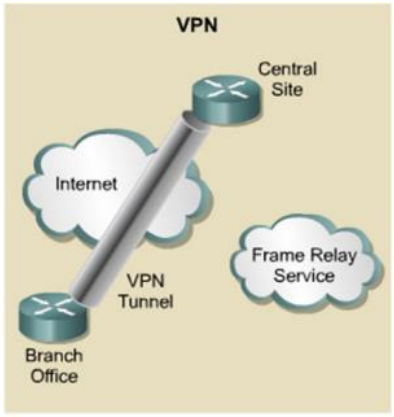
Certificates

- Used in authentication
- RSA uses digital certificates to authenticate peers
- The sender derives a hash based on the authentication key and identity information
- It encrypts this hash with its private key, this will act as a digital signature
- The signature is combined with a digital certificate, which includes the public key for decripting it
- At the receiver, the encrypted hash is decrypted using the public key of the sender
- If the decrypted hash matches the recomputed one, the signature is genuine
- The process happens in both directions to authenticate both devices

18. The protection of the traffic traversing public networks, VPNs in the different layers, IPSec, SSL

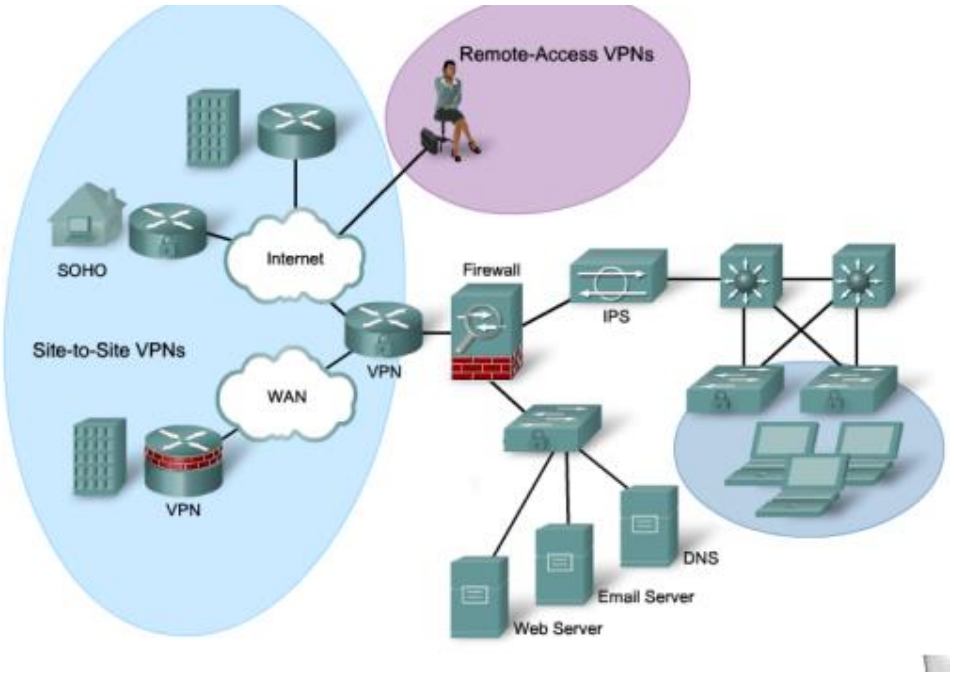
- VPN Benefits:
- Cost Savings
- Security
- Scalability
- Compatibility



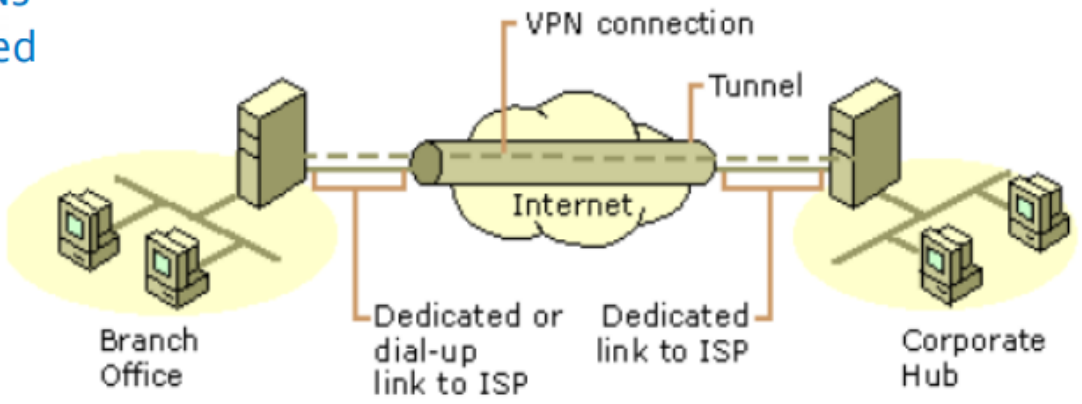


- VPN connects two endpoints over a public network to form a logical connection
- L2, L3, L4, L7
- A delivery header is added in front of the payload to get it to the destination site

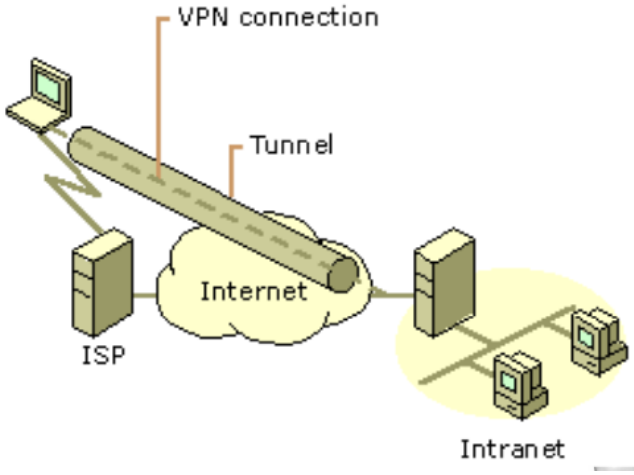
- Site-to-site VPN
- Remote access VPN



Two or more LANs are interconnected
The hosts send „normal" IP packets, they are unaware of the VPN
The traffic goes through a VPN gateway



Client-server connection
Client application is needed



Tunneling

- A tunnel is a mechanism used to ship a foreign protocol across a network that normally wouldn't support it.
- Using the infrastructure of a network we carry another datastructure of it.
- There are tunneling protocols that support some security service, others can only do it with other protocols.
- Hide the infrastucrutre below
- Decrease the hop number

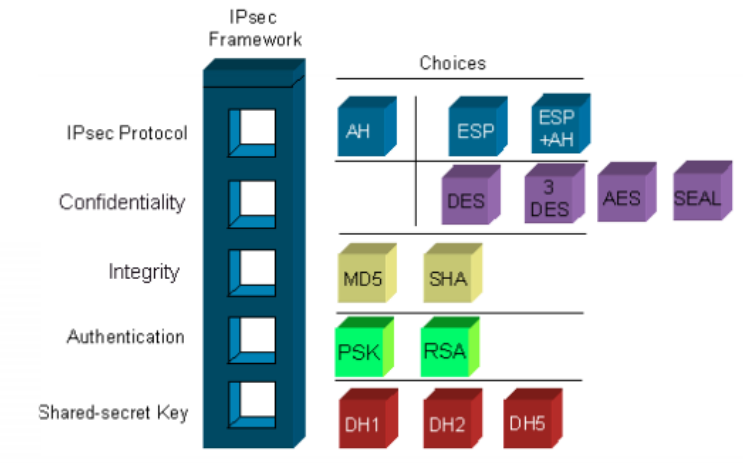
Examples:

- GRE: does not provide any security mechanism
- L2TP: authentication for users, encryption is not supported
- IPsec: authentication of devices, encryption and integrity is provided, does not authenticate users

GRE

- General Routing Encapsulation (tunnelling)
- GRE supports multiprotocol tunneling. It can encapsulate multiple protocol packet types inside an IP tunnel. (It can transport IP, IPv6, PPP, Frame-Relay packets, etc.)
- GRE also supports IP multicast tunneling. Routing protocols that are used across the tunnel enable dynamic exchange of routing information in the virtual network
- GRE does not provide encryption. If that is needed, IPsec should be configured.

IPSec



Protocols

AH – Authentication Header

- Authentication
- Integrity
- Traffic is unencrypted
- A checksum is computed on the entire packet and stored in this AH Header, even the newly added IP header, which makes AH incompitable with NAT
- **Security Parameter Index(SPI)**: It is an identifier that indicates to the receiver how to interprete the packet, what algorithms and keys should be used. AH assumes that the peers already negotiated all the parameters before with the help of ISAKMP/IKE protocol.
- **MAC**: Calculated hash value for the whole packet.

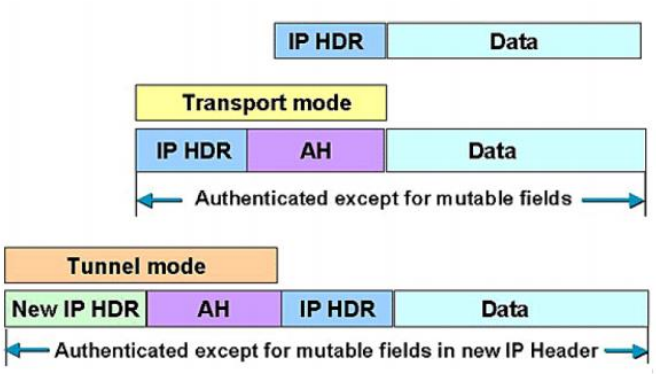
Authentication without encryption

- Data are public, we want to make sure about the origin of the data (company's website).
- Encrypting data is not so important
- Encryption is carried out below or above the IP layer.
- Encryption would give a much higher overhead to the resources.

ESP – Encapsulating Security Payload

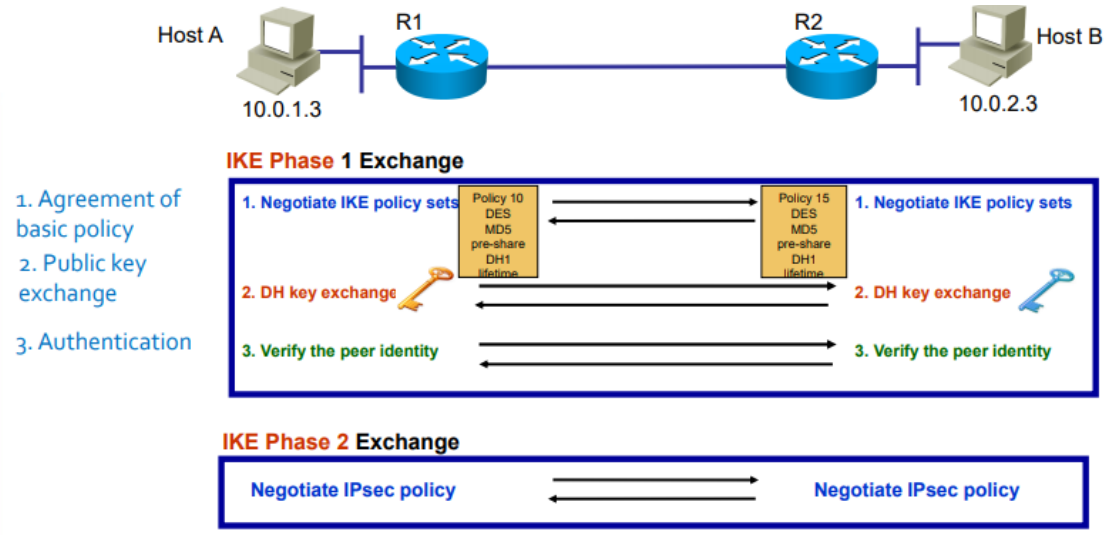
- Encryption
- Authentication
- Integrity
- Anti-replay
- Traffic is encrypted
- ESP is used to encrypt TCP/UDP header, Data and ESP trailer to provide confidentiality
- The ESP Client signs the ESP header, TCP or UDP header, Data and ESP trailer to prevent tempering
- **SPI** identifier indicates to the receiver how to interprete the packet, what algorithms and keys should be used. ESP assumes that the peers already negotiated all the parameters before with the help of ISAKMP/IKE protocol.
- **Seuence number** –for anti-replay

- **MAC** – optional



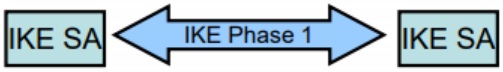
- An SA is a basic building block of IPsec.
- Security associations are maintained within a SA database (SADB), which is established by each device.
- A VPN has SA entries defining the IPsec encryption parameters as well as SA entries defining the key exchange parameters

Key exchange

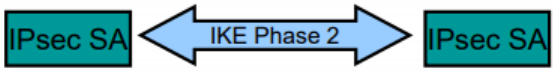


IPSec operation

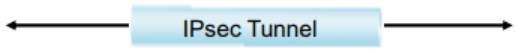
1. host A sends “interesting” traffic to host B.
2. R1 and R2 start to negotiate IKE SA, authenticate each other and set up a secure channel.



3. R1 and R2 start to negotiate IPsec parameters, and set up secure IPSec tunnel.



4. The tunnel is ready communication can start.



5. IPsec tunnel is terminated.

IPSec VPN configuration

Task 1: Configure the ISAKMP policy for IKE Phase 1
Task 2: Configure the IPsec Policy for IKE Phase 2
Task 3: Configure a Crypto Map for the IPsec Policy
Task 4: Apply the IPsec Policy
Task 5: Verify the IPsec Tunnel is Operational

SSL – Secure Socket Layer

- Used to create remote access VPN tunnel
- When a client negotiates an SSL VPN connection with the VPN gateway, it connects using Transport Layer Security (TLS)
- TLS is the newer version of SSL and sometimes refered to as SSL/TLS.
- Compared to IPSec, it is less secure but easier to deploy

SSL Protocol stack

- makes use of TCP (reliable end to end data transfer)
- adds security features
    - reliable and secure end to end data transfer
- SSL is not a single protocol
    - two-layers of protocols

SSL concepts

- **SSL session**
    - an association between client and server
    - define a set of cryptographic parameters created by the Handshake Protocol
    - may be shared by multiple SSL connections
- **SSL connection**
    - a temporary, end-to-end, secure communication link
    - associated with an SSL session
    - A session is used several times to create connections
- **Session vs. Connection**
    - Sessions are used to avoid expensive negotiation for crypto parameters for each connection
- **Both are characterized by several parameters**
    - that define a session state or connection state

Session state parameters

- **Session identifier**
    - chosen by server
- **Peer certificate**
    - certificate of the peer entity (server's if the entity is client, client's if the entity is server)
    - may be null (which is the likely case for server)
- **Compression method** (to be deprecated in TLS v1.3)
    - algorithm used for compression
- **Cipher Specification**
    - bulk data encryption algorithm (AES, etc.)
    - hash algorithm used in MAC calculation (MD5 or SHA-1 or SHA-2)
- **Master Secret**

    - 48-bytes secret shared between client and server
- **Is resumable**
    - a flag that is set if the session can be used later for new connections

Connection state parameters

- **Random numbers**
    - server and client exchange
    - used as nonces during key exchange
- **MAC secret**
    - secret key used for MAC operations
    - Separate for server and client
- **conventional encryption keys**
    - Separate for server and client
- **initialization vector**
    - if CBC mode is used 41 SSL Record Protocol

SSL Record Protocol

- uses connection parameters
- provides **confidentiality and integrity**
- also fragments (into 214 bytes chunks)
- optionally compresses data
- confidentiality
    - AES, IDEA, DES, 3DES, RC4, etc.
- message integrity
    - using HMAC with shared secret key

Change Cipher Spec Protocol

- very simple protocol
- the new state established by the handshake protocol is a pending state
    - that is, it is not yet valid
- change cipher spec protocol (actually a single command exchanged between client and server) makes this pending state the current one
    - connection parameters change after that
- will see its use in the handshake protocol

Alert Protocol

- conveys SSL-alerts to peer entity
- secured using the record protocol (if any)
    - and with current connection state parameters
- each message is two bytes
    - one byte for level (severity)
        - warning (connection may resume) or fatal (connection is terminated)
    - one byte for the alert code
        - unexpected message, bad record MAC, decompression failure
        - handshake failure (no common ground), illegal parameters (inconsistent or unrecognized parameters)
        - no certificate, bad certificate, unsupported certificate, certificate revoked, certificate expired, certificate unknown

Handshake Protocol

- The most complex part of SSL
- Allows server and client:
    - to authenticate each other
    - to negotiate encryption and MAC algorithms
    - to create cryptographic keys to be used
    - in general, to establish a session and then a connection
- handshake is done before any data is transmitted
    - so cannot assume a secure record protocol
- a series of messages in 4 phases
    1. Establish Security Capabilities
    2. Server Authentication and Key Exchange
    3. Client Authentication and Key Exchange
    4. Finish

19. Securing Local Area Networks: The types and operations of the L2 attacks and the possibility of the defense

CAM Table attack

Attack

- During basic switch operation, as the switch receives packets it fills up the CAM table with ports and associated mac addresses
- In a CAM table attack, the attacker will send packets with bogus MAC addresses from one of the ports with an attack tool, which fill up the CAM table as they get added
- Because the table is full, the switch begins the flood the frames to all ports, similarly to broadcast
- The frames will also be sent to the attacker, who can access sensitive data

Prevention

- Countermeasure against CAM attacks is Port Security
- It has to be enabled on the individual interfaces
- It allows us to set the maximum number of mac addresses, manually configure mac address, and to learn connected mac addresses dynamically on the port
- Different violation modes can be configured as a reaction
    - Protect: stops forwarding traffic
    - Restrict: also send system log message and increases violation counter
    - Shutdown: also shuts down the port
- Aging for ports can also be configured, making secure addresses expire
    - Set the aging time
    - Absolute type: all addresses age out after the time
    - Inactivity type: addresses only age out only if there is no traffic within the time

Attack the Root

Attack

- Relevant when we have switches in STP
- The root switch within the spanning tree is attacked
- The attacker can add a new switch and make it the root
- Most of the traffic in the network goes through this root switch
- An attacker can see this traffic using a packet sniffer

Prevention

- **BPDU Guard** protects PortFast enabled ports and against new switched added to the topology
    - PortFast enabled interfaces enter STP forwarding state immediately
    - Should be applied to all PortFast enabled and end-user ports
- **Root Guard** helps secure the root role within the STP
    - Should be applied on all interfaces that connect to swiches that shoudl not became root bridge
    - It can help prevent a new switch from trying to claim the root role with malicious intent
    - If detected it moves that port into a root-inconsistent state ---listening
- **Loop guard** prevents layer 2 loops within the STP
    - When a non designated port with loop guard enabled stops receiving BPDUs, it is put into an inconsistent blocking state instead of listening/learning/forwarding state
    - Apply to all ports that are or can become non-designated

- **Disable DTP**

DTP and VTP attack

DTP

- Helps manage automatic trunk negotiation on link between switches

VTP

- Automates the propegation of VLAN information, such as additions, deletions and name changes
- Switches sycnhronize their configuration based on the received information
- Works based on clients and servers, servers can edit vlans, send advertisements, and save the configuration
- VTP messages are sent as multicast, every time there is a change or every 5 minutes by default
- VTP Pruning can help prevent flooding unneccesarry traffic to switched that do not have members in the specific VLANs
- VTP domains can be protected by configuring a VTP password, which is propagated in the domain in summary advertisments

Attack

- A new switch can be connected and its interface set to trunk because DTP is enabled by default
- The attacker can use this switch to act as a server, set a domain name (putting all switches in a domain), and propagate VLAN information to make malicious changes

Prevention

- Shutdown unused ports, use Port Security
- Disable DTP
- Configure Access mode
- VTP Transparent mode(does not syncronise, changes only on the local switch) and Authentication

VLAN attack

VLAN Hopping

- Attacker gains access to VLANs he should not be able to

VLAN Double-Tagging

- The attacker tag the frame not only with their own, but also the target VLAN
- The first switch will remove the first tag, which is that of the attacker's and forward the frame
- The first switch doesnt retag the frame because native traffic is not retagged
- The second switch will see the frame tagged with the target VLAN and forward it accordingly

Prevention

- Disable DTP
- Manually enable trunk links
- Set the native VLAN to something other than VLAN 1
- Disable unused ports and put them in an unused VLAN

Private VLAN port types

- Promiscuous ports: communicate with all ports
- Isolated ports: communicate only with the promiscuous ports

- Community ports: communicate only with ports in the same community and promiscuous ports

DHCP attack

DHCP Starvation

- Send DHCP requests to consume all the available IP addresses

Prevention

- Port Security
- 802.1x authentication
- DHCP snooping rate limit for interfaces (e.g. max 10 dhcp msg per second)

DHCP Spoofing

- Use a rouge server the service DHCP clients in place of the legit server by servicing them sooner, serve them fake configuration parameters to achieve malicious goals like packet sniffing/dns attack

Prevention

- **DHCP Snooping** trust port
    - Ports can be marked as trusted and untrusted, legit dhcp server on the trusted port
- 802.1x authentication
- Port Security
- Shutdown unused ports

ARP attack

ARP

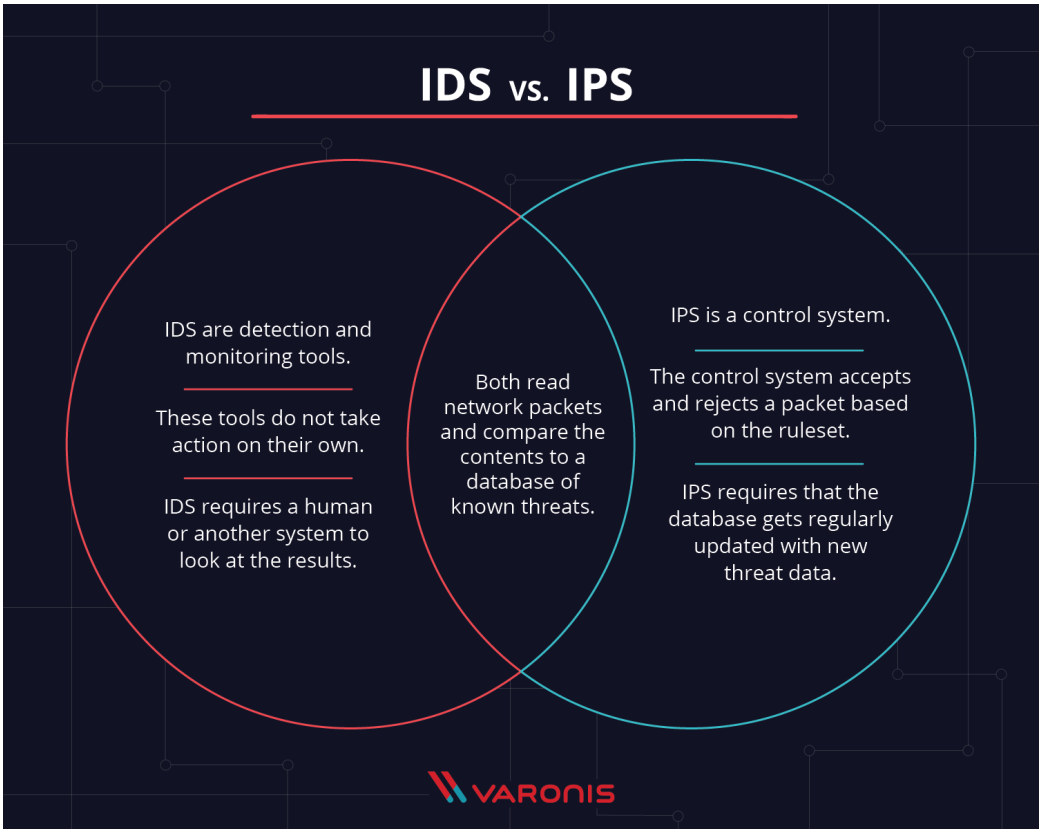
- Devices within a network use Address Resolution Protocol to map the IP addresses to MAC addresses
- ARP requests are sent, and the host with matching IP will respond
- The attacker can send fake ARP replies and map its own MAC address to IP addresses to receive the traffic
- There is no security mechanism that allows switches to verify the source of MAC addresses

Prevention

- **Dynamic ARP Insepection** intercepts all ARP requests and responses, and uses the DHCP snooping table which is built from DHCP requests to check if the ARP from the interface is within the binding, if not, its blocked
- It is configured by VLAN
- Interfaces can be trusted/untrusted
- **IP Source Guard (IPSG)** is very similar, but looks at every packet, not just ARP

- Port Security defends against CAM attacks and DHCP Starvation attacks
- DHCP snooping prevents rouge DHCP server attacks
- Dynamic ARP inspection prevents current ARP attacks

20. The operation and characteristics of Intrusion Detection Systems (IDS) and Intrusion Preventions Systems (IPS)



Intrusion Detection Systems

- **Monitoring for attacks**
- Works passively
- Requires traffic to be mirrored, traffic does not pass through if it is not
- **Advantages**
    - No impact on network
    - No network impact on sensor failure
    - No network impact on sensor overload
- **Disadvantages**
    - Cannot stop the violation, only detects
    - More vulnerable to network security evasion

Intrusion Prevention Systems

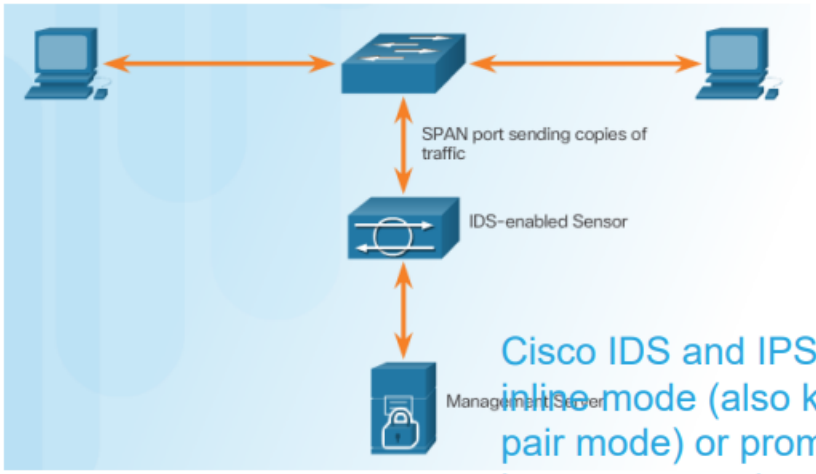
- **Detect and Stop attacks**
- Implemented in an inline mode
- Monitors layer 3 and 4 traffic
- Can stop single packet sttacks from reaching target
- Immidiate response
- **Advantages**
    - Stops attacks
- **Disadvantages**
    - Has impact on network, especially sensor issues

	Advantages	Disadvantages
Host-Based IPS	• Provides protection specific to a host operating system • Provides operating system and application level protection • Protects the host after the message is decrypted	• Operating system dependent • Must be installed on all hosts
Network-Based IPS	• Cost effective • Operating system independent	• Cannot examine encrypted traffic • Must stop malicious traffic prior to arriving at host

	Advantages	Disadvantages
Network IPS	• Is cost-effective • Not visible on the network • Operating system independent • Lower level network events seen	• Cannot examine encrypted traffic • Cannot determine whether an attack was successful

Modes of Deployment

Promiscuous Mode



Cisco IDS and IPS sensors can operate in inline mode (also known as inline interface pair mode) or promiscuous mode (also known as passive mode).

Inline Mode

Signature

A **Signature** is a set of rules that an IDS and IPS use to detect typical intrusion activity

- Type
- Trigger (alarm)
- Action

Types

- **Atomic**
  - simplest signature, consists of a single packet, activity or event that is examined for match. If yes, alarm is triggered
  - consumes minimal resources
  - easy to identify or understand
- **Composite (stateful signature)**
  - This type of signature identifies a sequence of operations ditributed across multiple hosts over an arbitrary period of time
  - Maintain state information
  - Several piecec of data to match
  - Event horizon – cannot maintain state information indefinitely long, after initial signature component is detected

Signature File

- As new threats are identified, new signatures must be created and uploaded to an IPS.
- A ginature file contains a package of network signatures

Pattern-Based Detection

Example	Detecting an Address Resolution Protocol (ARP) request that has a source Ethernet address of FF:FF:FF:FF:FF:FF.	Searching for the string "confidential" across multiple packets in a TCP session.

Advantages	Disadvantages
• Easy configuration • Fewer false positives • Good signature design	• No detection of unknown signatures • Initially a lot of false positives • Signatures must be created, updated, and tuned

Anomaly-Based Detection

Example	Detecting traffic that is going to a destination port that is not in the normal profile.	Verifying protocol compliance for HTTP traffic.

• Simple and reliable • Customized policies	• Generic output • Policy must be created

Policy-Based and Honey Pot-Based Detection

Example	Detecting abnormally large fragmented packets by examining only the last fragment.	A Sun Unix host sending RPC requests to remote hosts without initially consulting the Sun PortMapper program.
Policy-based Detection	• Easy configuration • Can detect unknown attacks	• Difficult to profile typical activity in large networks • Traffic profile must be constant
Honey pot-based Detection	• Window to view attacks • Distract and confuse attackers • Slow down and avert attacks • Collect information about attack	• Dedicated honey pot server • Hot pot server must not be trusted

Understanding Alarm Types:

Alarm Type	Network Activity	IPS Activity	Outcome
False positive	Normal user traffic	Alarm generated	Tune alarm
False negative	Attack traffic	No alarm generated	Tune alarm
True positive	Attack traffic	Alarm generated	Ideal setting
True negative	Normal user traffic	No alarm generated	Ideal setting

Summary of Action Categories:

Category	Specific Alert
Generating an alert	Produce alert
	Produce verbose alert
Logging the activity	Log attacker packets
	Log pair packets
	Log victim packets
Dropping or preventing the activity	Deny attacker inline
	Deny connection inline
	Deny packet inline
Resetting a TCP connection	Reset TCP connection
Blocking future activity	Request block connection
	Request block host
	Request SNMP trap
Allow the activity	This action will permit the traffic to appear as normal based on configured exceptions. An example would be allowing alerts from an approved IT scanning host.