Introduction to Network Security

Segurança em Redes de Comunicações

Mestrado em Cibersegurança

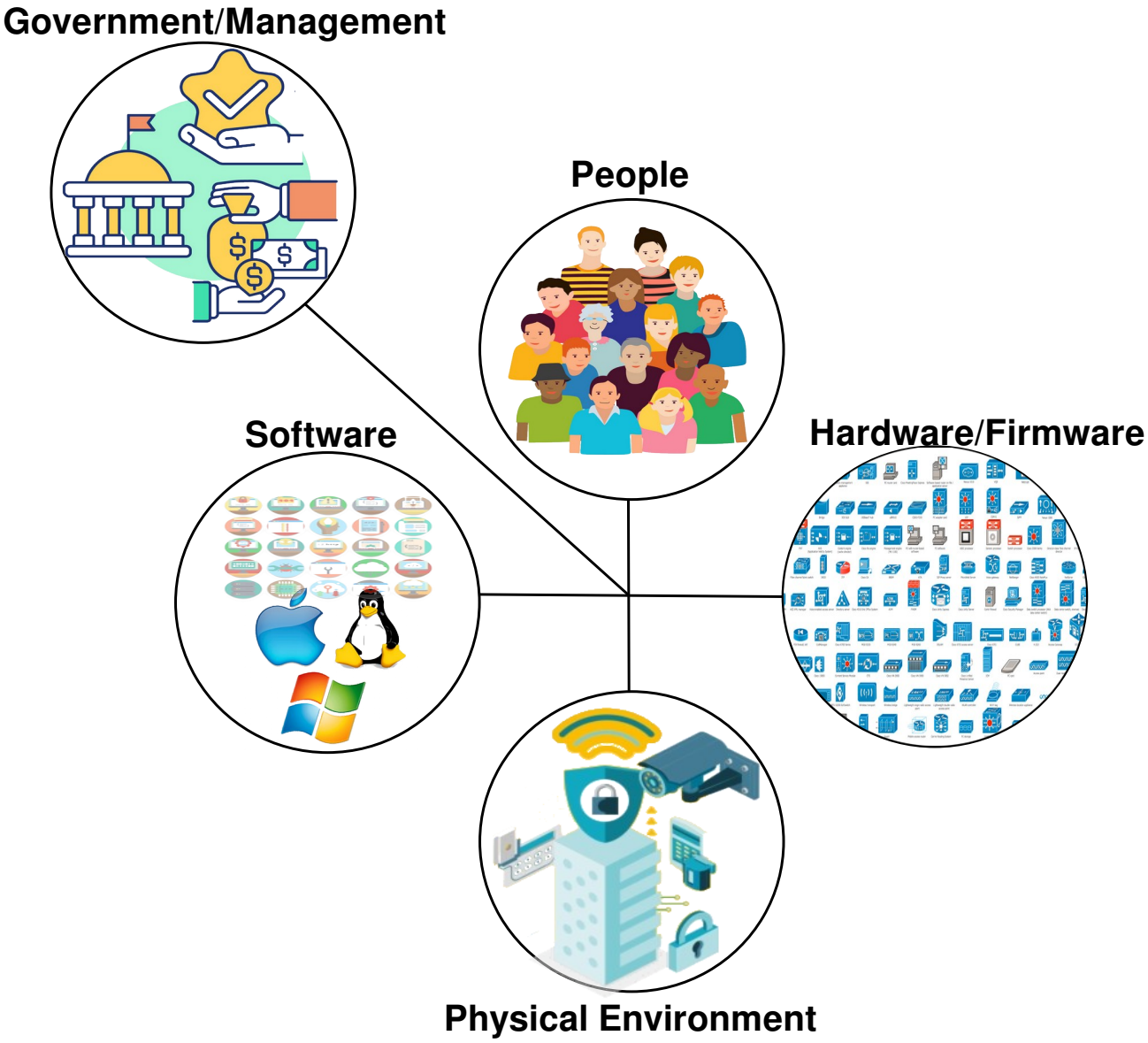
Mestrado em Engenharia de Computadores e Telemática

DETI-UA

universidade de aveiro

deti.ua.pt

Network Security Pillars



Network Operations Center (NOC)

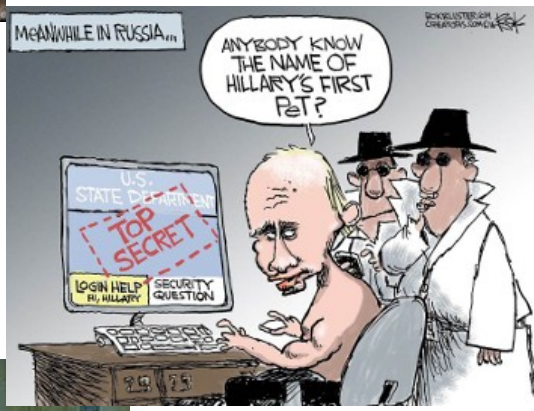
- Security competences of a NOC in an organization:
  - Network resilience and high-availability
  - Network/services segregation
  - Network devices, terminals and server/services deployment
    - Firmware/Software install, update and patch
  - Security policies deployment
    - Firewalls, IDS/IPS, etc...
  - Data acquisition
  - Threat mitigation
    - Firewall rules (by request)
    - Device isolation/deactivation
  - Forensics
    - Done after an attack
    - Gather evidences for judicial purposes
    - Gather additional data to improve future prevention/detection/response, data acquisition and threat mitigation (NDR by NOC).

Security Operations Center (SOC)

- Competences of a SOC in an organization:
  - Prevention and detection of attacks
    - Monitor network and services (with SIEM)
    - Detect vulnerabilities (with vulnerability scanning tools)
    - Detect malicious activities (with SIEM)
    - Detect anomalous behaviors (with SIEM)
      - may not be malicious!
  - Investigation
    - Analyze the suspicious activity to determine/characterize the threat
    - Evaluate how deep the threat has penetrated the network/systems
  - Response
    - Deploy counter measures based on known playbooks
    - Deploy emergency measures when threat do not match a known response playbook
  - Forensics
    - Done after an attack
    - Gather evidences for judicial purposes
    - Gather additional data to improve future prevention/detection/response, data acquisition and threat mitigation (NDR by NOC).
- Nowadays commonly operated independently of the Network Operation Center (NOC).
- Should be integrated with NOC.
  - For network/services segregation and resilience, data acquisition and threat mitigation.

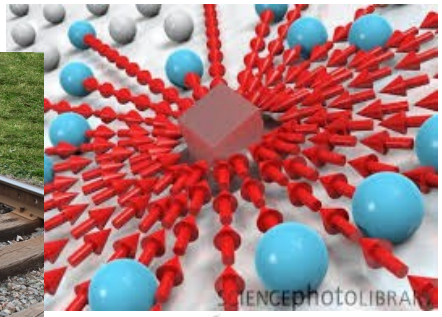
Type of Attacks (1)

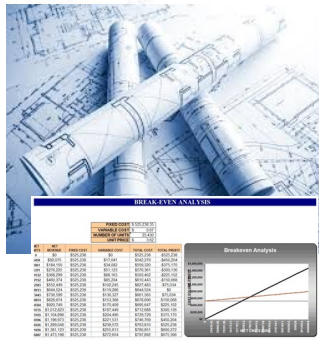
- Objectives:
  - Fun and/or hacking reputation
  - Political purposes
  - Military purposes
  - Economical purposes
  - Other?
- Technical objectives:
  - Operation disruption
  - For data interception
  - Both
    - Disruption to intercept!
    - Intercept to disrupt!



Type of Attacks (2)

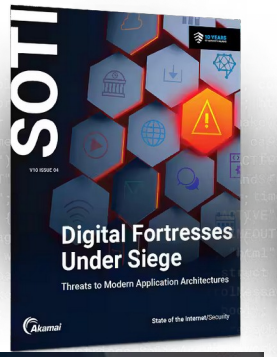
- Technical objectives:
  - Operation disruption.
    - (Distributed) Denial-of-Service.
  - Resources hijack.
    - Spam,
    - Crypt-currency mining/masternodes,
    - Platform to other attacks!
  - Data interception/stealing.
    - Personal data
      - As final goal,
      - Or as tool to achieve more value information!
    - Technical data,
      - Usually used to achieve more value information!
    - Commercial data
      - Digital objects, financial and/or engineering plans, ...
- Disruption may be used to achieve interception!
- Interception may me used to achieve disruption (operational or commercial)!

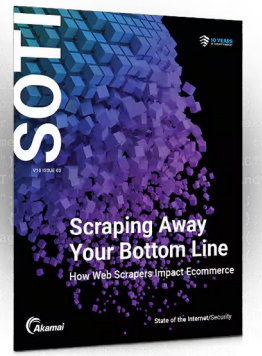


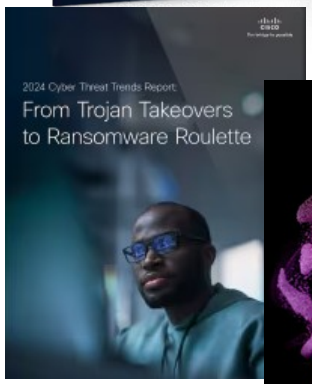


Security Reports

- Akamai State of the Internet Reports
- Cisco Cyber Threat Trends Report
- Checkpoint Cybersecurity report
- Deloitte Cyber Threat Trends report
- Fortinet Application Security Report
- Cloudflare State of Application Security
- Paloalto The State of OT Security
- Paloalto Incident Response
- NSA Cybersecurity Year in Review







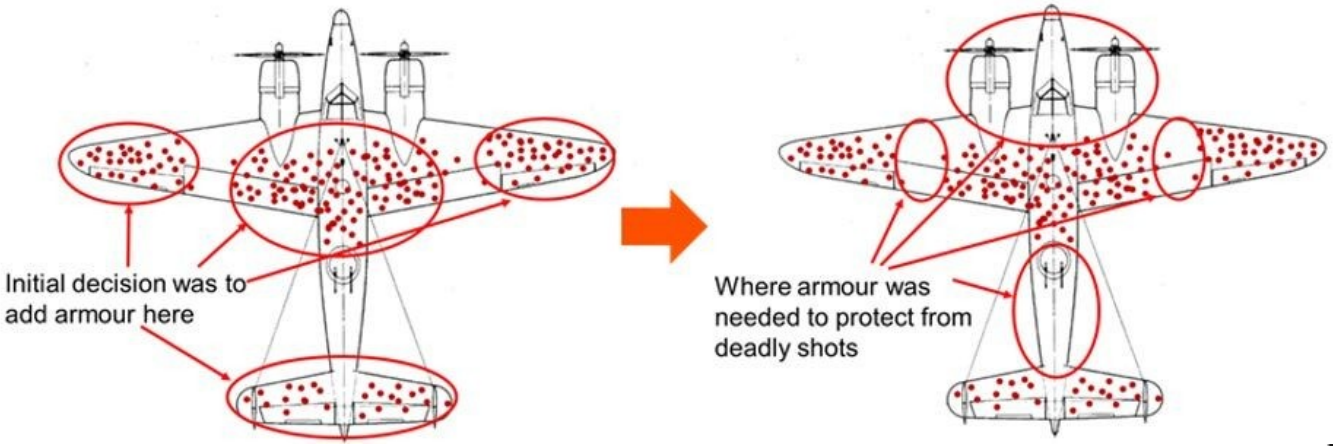
universidade de aveiro

More on Security Reports

- Identify threats with solutions, recommend to implement known solutions and good practices.
- “Hint” to the existence of many unknown threats:
  - Actors.
  - Technological (zero-day)
  - Levels
    - Network and software.
- Commercial frameworks design to (try to) solve unknown threats.
  - No concrete results or analysis of performance!

Observation Bias

- Data is captured and analyzed in a way that confirms pre-existing observations and beliefs.
  - Other data is not considered.
- This impacts how data is collected, analyzed, and acted upon in cybersecurity.
  - Limit data collection and analysis.
  - Solutions only to visible problems.
  - Unknown threats remain hidden and unsolved!
- Only visible attacks (successful or not) are considered relevant.
- **Unseen/stealth attacks are not considered!**
- WW2 planes ana

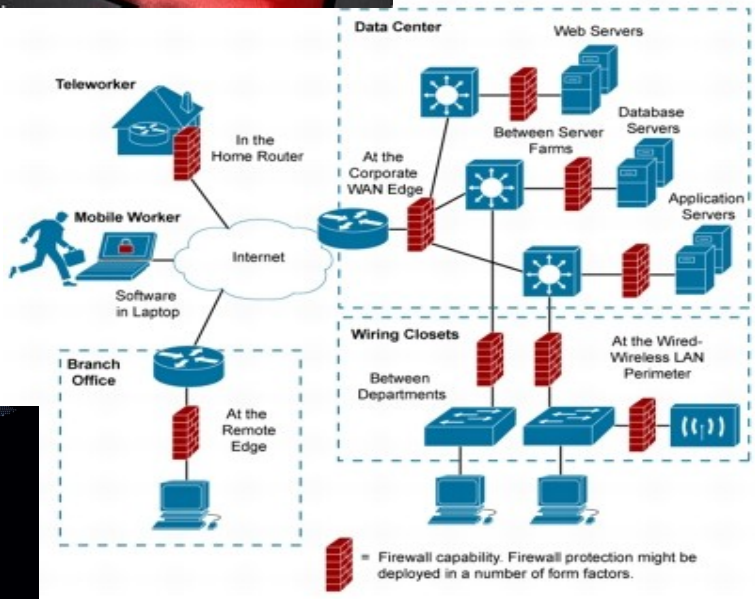


Cyber-Physical Security (non-network)

- General Security
  - Doors, Locks, Alarms, Personal, Sensors, etc...
- Human train for internal and external interaction.
- Access and movement policies
  - Inside premises and near-premises.
- Environment control redundancy and monitoring
  - Temperature, AC, Humidity, Sound, Smoke, etc...
- Power redundancy and monitoring
- Radio awareness (spectrum monitoring) and suppressors (Faraday cages)
- ...

Traditional Defenses

- Vulnerability patching.
- Firewalls
  - Centralized.
  - Distributed.
- Intrusion Prevention and Detection Systems (IDS/IPS).
- Antivirus.



- **All rely on previous knowledge of the threat and/or problem!**

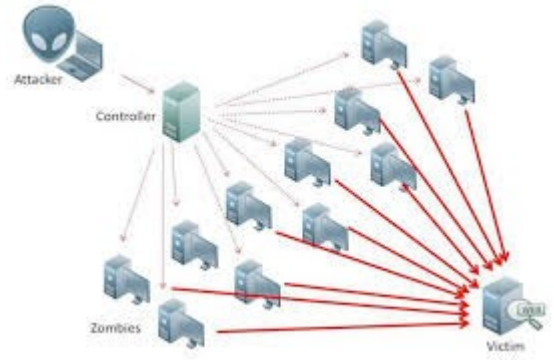
Advanced Persistent Threats

- When an attacker uses sophisticated methods.
- Focuses on specific organizations, exploring **new vulnerabilities** with **new tools**.
  - Usually previously tested with known security tools and systems.
- The attacker presence within the network have long-term goals.
- The objective is to steal, disrupt or both.
  - Large impact goals!
- Activity is stealth
  - Learns licit behaviors,
  - Perform mimic attacks,
  - Adjusts tactics based on defenses.
- May use multiple attack vectors and communication channels.
  - Alternative communication technologies (Bluetooth, Zigbee, LoRa, etc…).
  - Licit services as C&C and exfiltration vectors (DNS, Webservices, Cloud services, etc…).

“Intelligent” Defenses

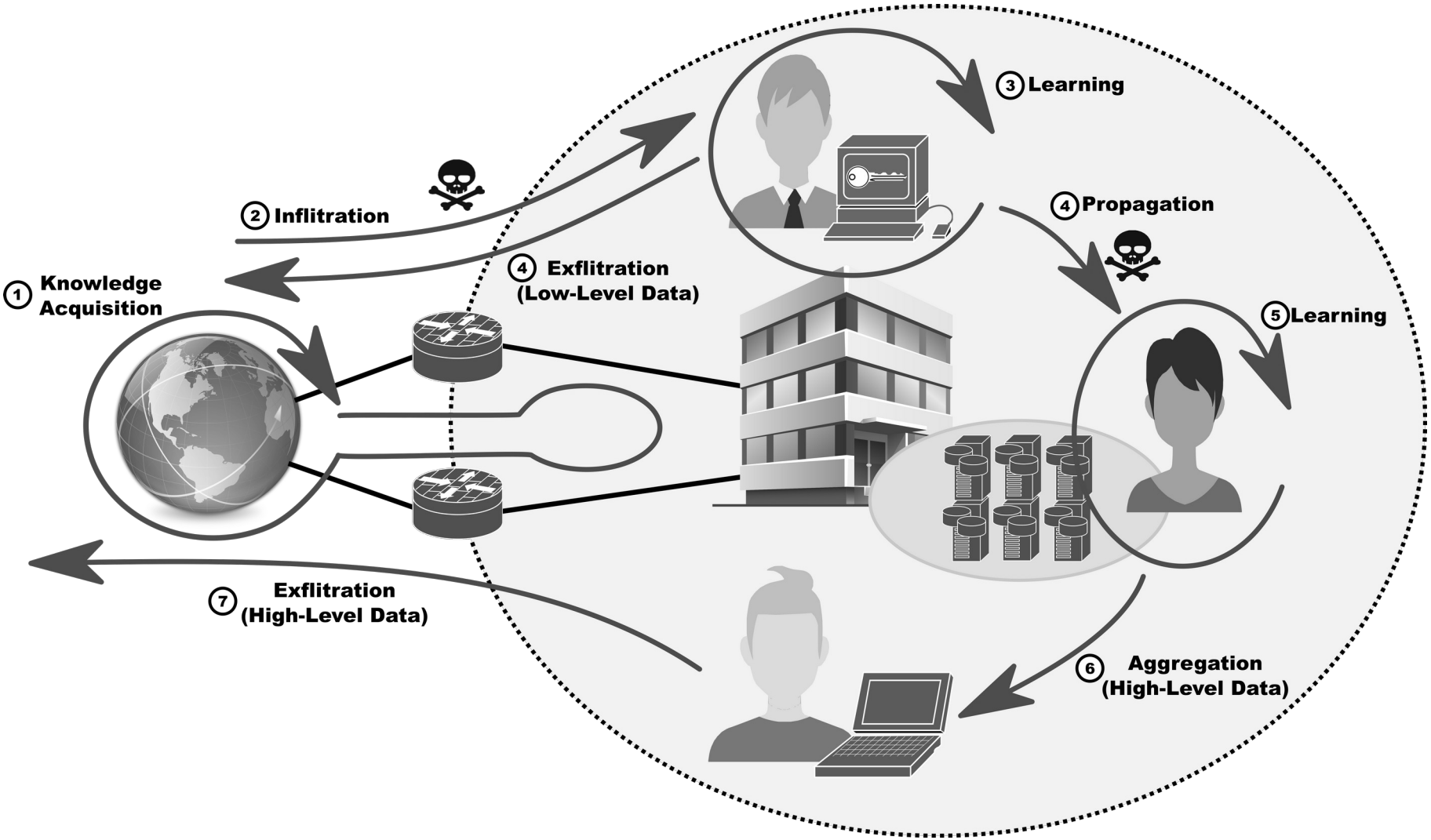
- Detection of unknown threats and/or problems.
  - In time to deploy counter-measures.
- Application of Big Data and Data Science techniques to network ans systems monitoring data.
- Some traditional solutions start to incorporate AI into their equipment
  - E.g., Palo Alto Network Firewalls, Cisco Appliances, …
- Still limited to manufacturer based solutions and localized data.
- Still limited in scope.
  - Obvious threats vs. Stealth threats.
- Optimal deployment requires an overall network and systems knowledge.
  - Network and Systems (Cyber) Situational Awareness.

Disruption Attacks

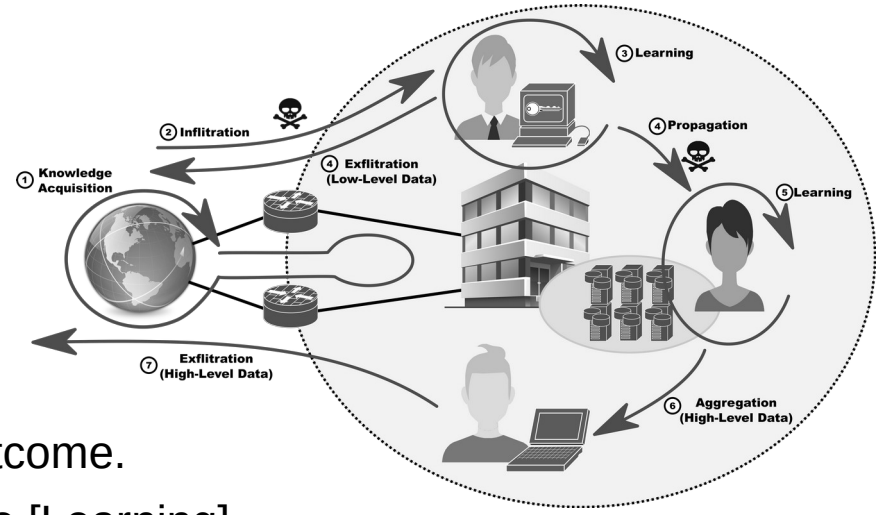


- Distributed DoS
  - Multiple slow/small devices generating traffic to a target
    - TCP vs. UDP
  - Purpose of disruption
    - By political/economical/"reputation"
    - Redirection to other service/location?
  - Solution at target
    - Load-balancers
    - For TCP, maybe its possible to survive making active (with licit client validation) session resets (server/firewalls)
      - White list solution, for completed session negotiation
    - For UDP/DNS, block requests for known external relay/redirection DNS servers (blocks attack amplification, IP target spoofing)
      - Doesn't work with large botnets and direct requests to target
  - Solution at source
    - Anomalous behaviors detection
      - Low traffic variations hard to detect
      - Time and periodicity changes are easier to detect
      - Destinations of traffic changes
      - With "really low" data rates is impossible to detect
- Denial of service by physical signal jamming
  - Pure disruption, or
  - Disruption to activate secondary channels (more easily compromised).
  - Solution
    - Detect, localized source and physically neutralize.
- Disruption of support services/utilities
  - Internet external connection, power, water, access roads, etc...

Attacks Phases



Attacks are Done Incrementally



- Escalation of goals and privileges.
  - Public knowledge opens doors to private information and access to protected domains [Infiltration].
  - The first illicit access to a protect domain may not provide a relevant outcome.
  - Attacker must acquire more knowledge [Learning].
  - The additional knowledge allows to access other secure domain zones/devices/data with increasing relevance [Propagation].
    - At any phase the attacker may require additional knowledge [Learning].
  - When a relevant outcome is acquired it must be transfered to outside of the protected domain [Exfiltration].
  - Direct exfiltration may denounce the relevant points inside of the secure domain.
    - The relevant outcome must be first transferred inside the protected domain to a less important point [Aggregation].
    - Attacker chooses a point that may be detected and lost without harm.

Technical Network Vulnerabilities

- Software
  - Applications
  - Frameworks/API
  - Protocols
  - Operating systems
    - Kernel, kernel modules, drivers, and base applications.
    - Configurations!
  - Low level code
    - CPU microcode, firmware, and BIOS/UEFI.
- Hardware
  - Physical tempering
  - Physical emissions
    - Electromagnetic emissions, sound, ...
  - Power instability, Electromagnetic Pulses (EMP), etc ...
- Known vs. unknown
  - CVE
  - IDS/IPS and antivirus databases

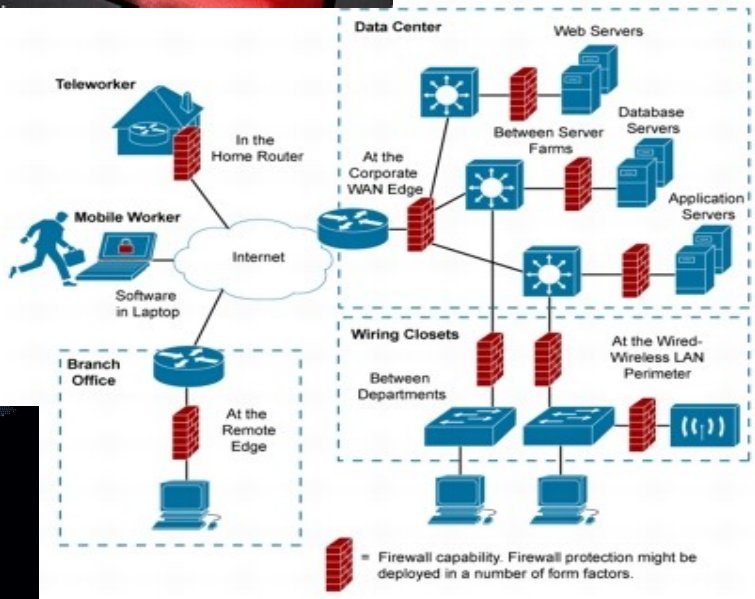
CVE

Common Vulnerabilities and Exposures

universidade de aveiro

Traditional Defenses

- Vulnerability patching.
- Firewalls
  - Centralized.
  - Distributed.
- Intrusion Prevention and Detection Systems (IDS/IPS).
- Antivirus.



- **All rely on previous knowledge of the threat and/or problem!**

“Intelligent” Defenses

- Detection of unknown threats and/or problems.
  - In time to deploy counter-measures.
- Application of Big Data and Data Science techniques to network ans systems monitoring data.
- Some traditional solutions start to incorporate AI into their equipment
  - E.g., Palo Alto Network Firewalls, Cisco Appliances, …
- Still limited to manufacturer based solutions and localized data.
- Still limited in scope.
  - Obvious threats vs. Stealth threats.
- Optimal deployment requires an overall network and systems knowledge.
  - Network and Systems (Cyber) Situational Awareness.

Infiltration Phase

- Licit machines must be compromised to implement the different attacks phases.
  - Ideally in a privileged “zone” of the network, and/or
  - With access credentials, and/or
    - User credentials, address(es), hardware key, etc…
  - With “special” software, and/or
  - Target data.
- May include the installation of software or usage of licit vulnerable software.
- May be remotely controlled (constantly or not).
  - Command and control (C&C).
- May have autonomous (AI) bots installed to perform illicit actions.
  - When remote C&C is not possible or subject to easy detection.

Remotely by Exploiting Licit Users

- Objectives:
  - Credentials acquisition.
  - Software insertion.
  - Ramsomware.
- Vectors:
  - E-mail and social networking
    - Phishing for credentials.
    - Office macros.
    - Binaries execution.
  - Downloadable software
    - Cracks.
    - Non-certified software stores.
    - …

Remotely by Attacker Actions

- Possible when network/systems have unpatched (unresolved) vulnerabilities.
  - Limited in time.
- Possible when network/systems are poorly configured/designed
  - Less limited in time.
  - Hard to perform discovery without detection by traditional defense systems.
    - Sometimes poorly configured/designed systems are not protected by adequate systems (if any).
- Usually not done first.
- Done after acquiring some credentials/privileges from licit users.
  - Using direct connections/services.
  - Easier to hide (stealth attacks) by having reduce activity or mimicking licit usage.

Locally by Physical Interaction

- Objectives:
  - Traffic interception.
  - Local network access to exploit vulnerabilities.
  - Direct access to machine.
- Vectors:
  - Ethernet ports at public/unprotected locations
    - With VLAN separation
    - Without VLAN separation
    - Protected by 802.1X
  - Network taps at public/unprotected locations
  - Fake access points.
    - Rogue access points
  - Low security in IoT devices/network (Bluetooth, Zigbee, Thread)
  - Network devices access
    - Unprotected serial/console ports, USB ports, etc...
  - USB ports (short time access)
    - Long time objectives
      - Trojan/root kits injection.
    - Short time objectives
      - Device data acquisition (contacts, messages, sms, etc...)
  - Sitting down at a terminal or with a device!
  - Other?

Propagation Phase

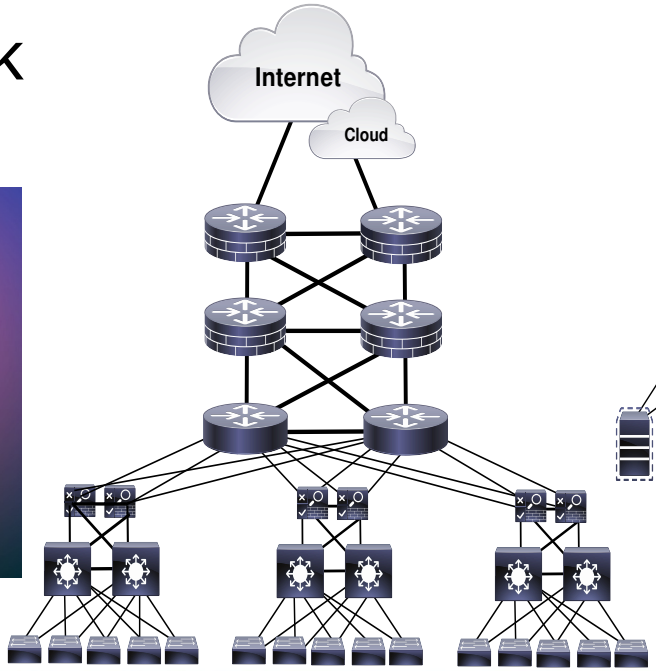
- Done using a mixture of methodologies:
  - Credentials exploitation.
    - Direct usage or by using allowed applications.
  - Impersonating users and systems.
    - Similar to credential exploitation but more advanced based on acquired knowledge (licit behavior).
    - Requires time to learn and mimic licit behavior.
      - Time patterns, traffic patterns, application patterns, etc...
  - Vulnerability exploitation.
    - Inside a protected domain systems are many times considered in a secure zone.
    - Less maintained and legacy OS/applications may be required to run (no patching).
    - Broader range of vulnerabilities

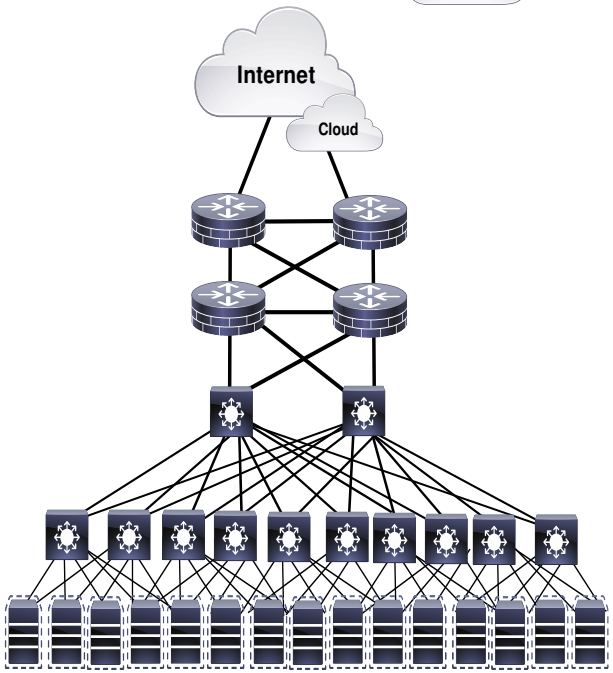
Aggregation and Exfiltration Phase

- Data transferred from machine to machine.
- Internally [Aggregation] it can be done using existing channels.
- Externally [Exfiltration]
  - It can be done directly using existing channels.
    - File copy, email, file sharing, etc…
    - Can be detected.
  - It can be done hiding information within existing/allowed channels and licit communications.
    - Slower data transfer, harder (impossible?) to detect.
    - Examples:
      - Usage of steganography in photos (via social networking).
      - Usage of embed data in text and voice messages.
      - ...

Simple vs Complex Scenarios

- Small/medium network
- Large Network
- Datacenter
- Geographically distributed network





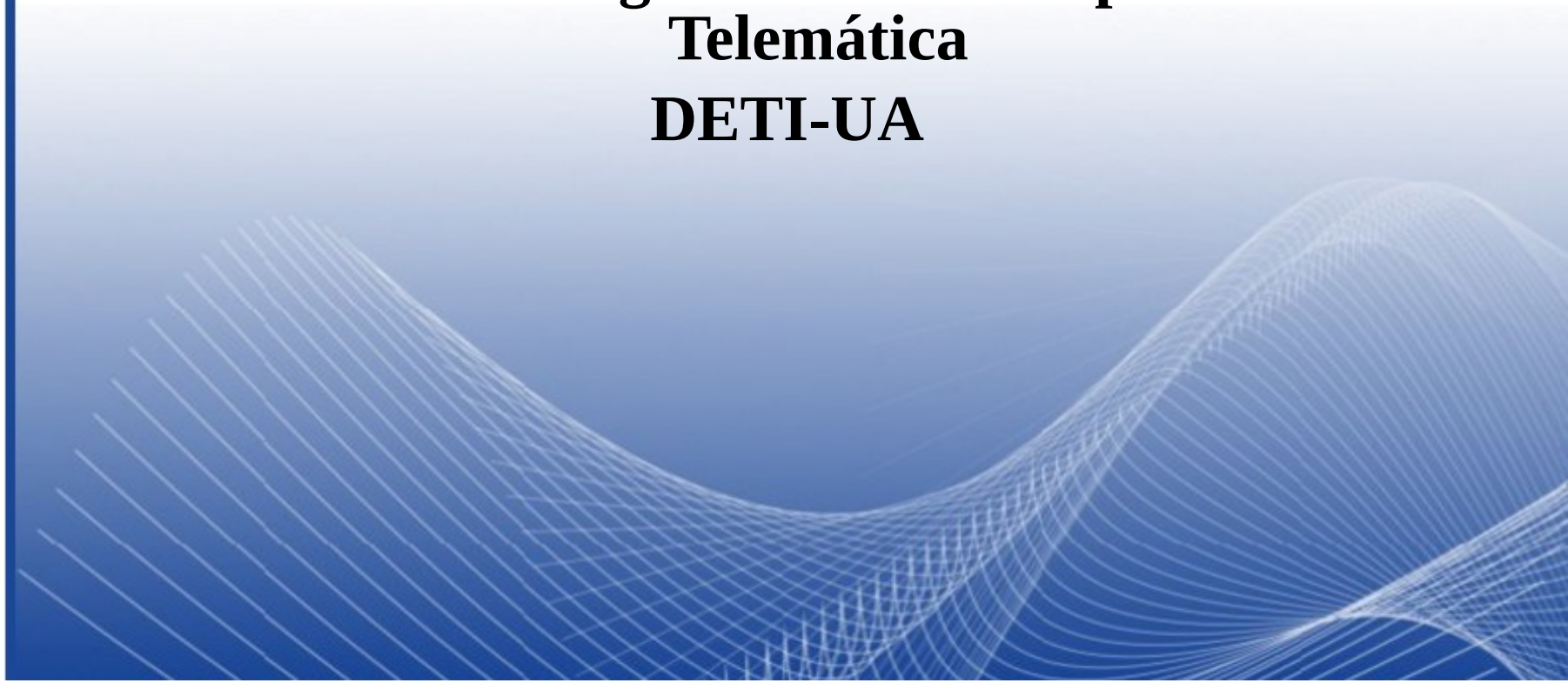
Corporate Network Topics

Segurança em Redes de Comunicações

Mestrado em Cibersegurança

Mestrado em Engenharia de Computadores e Telemática

DETI-UA



universidade de aveiro

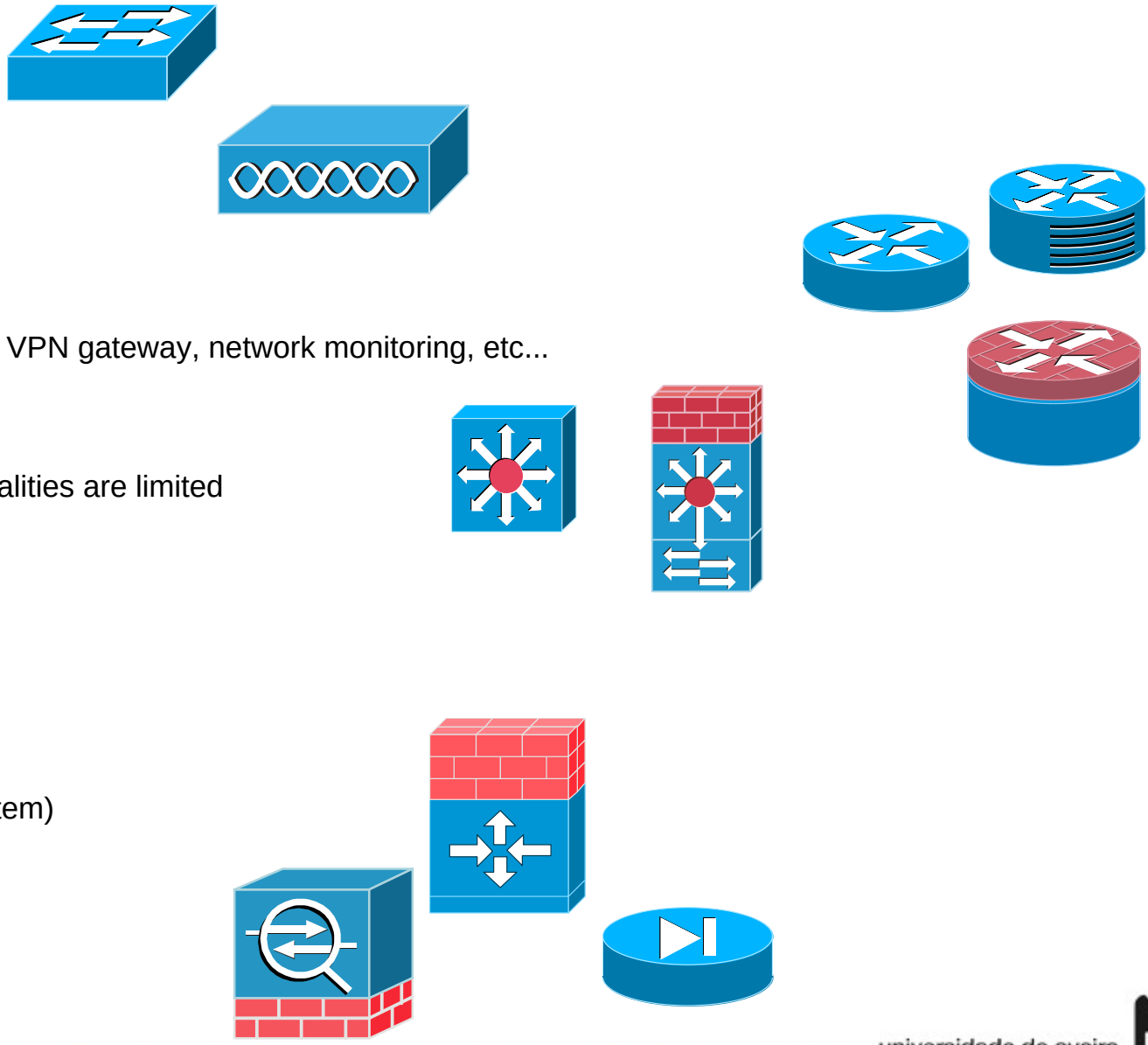
deti.ua.pt

Objectives of Network Design

- Network should be **Modular**
  - Support growth and change.
  - Scaling the network is eased by adding new modules instead of complete redesigns.
- Network should be **Resilient**
  - Up-time close to 100 percent.
    - If network fails in some companies (e.g. financial), even for a second, may represent millions of lost revenue.
    - If network fails in a modern hospital, this may represent lost of lives.
  - Resilience has costs.
    - Resilience level should be a trade-off between available budget and acceptable risk.
- Network should have **Flexibility**
  - Businesses change and evolve.
  - Network should adapt quickly.

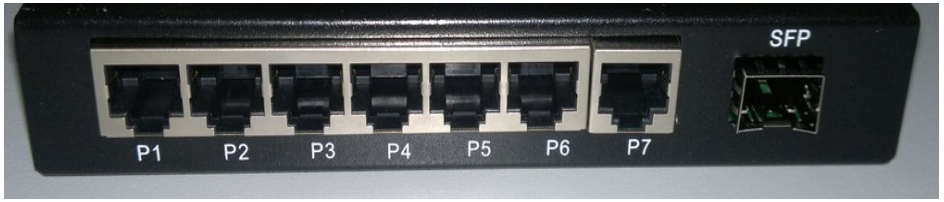
Equipments

- Switch
  - OSI Layer 2 inter-connection
  - Implements VLAN
  - Spanning-tree based routing
    - STP, RSTP, MSTP
  - Wireless Access Points
- Router
  - OSI Layer 3 inter-connection
  - Have extra functionalities like QoS, Security, VPN gateway, network monitoring, etc...
- L3 Switch
  - Switch+Router
  - Low-end and mid-end range routing functionalities are limited
  - High-end have full routing functionalities
  - Many have dedicated L2 routing hardware
- Router with switching modules
  - L3 Switch with full routing capabilities
- Security Appliance
  - Firewall
  - IDS/IPS (Intrusion Detection/Prevention System)
  - NAT/PAT
  - VPN Gateway
  - Services proxy

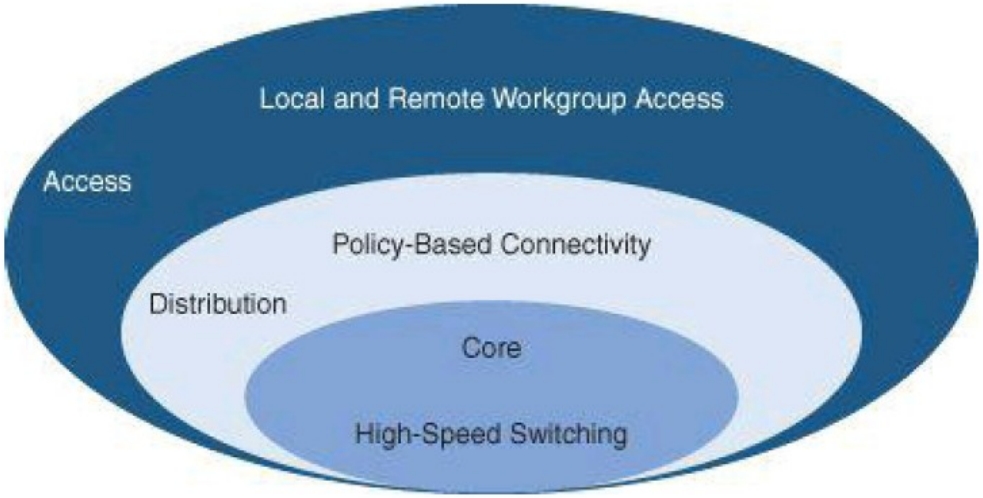


How to Choose the Equipments

- Type
  - L2 Switch, L3 Switch, Router + Switching module, Router, …
- Manufacturer
  - Reliability
    - (Expected) Maximum MTBF (mean time between failures) as possible.
    - Depends on multiple factors:
      - Hardware/Electronics redundant architectures, inherent quality, environmental constrains, etc...
  - Price
    - Usually (not always), a lower price means lower reliability.
  - Assistance
- Range/Model
  - Processing/Commutation speed
    - Number of bytes/packets processed/commuted per second.
      - Lower than the sum of all ports speed.
  - Software version
    - Supported protocols and functionalities.
    - Determines also memory requirements.
  - Number of ports (and speed of ports)
    - Ethernet (10 Mbps, 100 Mbps, 1Gbps, 10Gbps, …)
    - Connectors
      - To copper or to fiber.
      - RJ-45, Small form-factor pluggable (SFP), Enhanced small form-factor pluggable (SFP+) …
    - With or without PoE (Power over Ethernet)
      - For VoIP phones, Access Points, etc...
  - Number of slots
    - For additional port/processing modules.

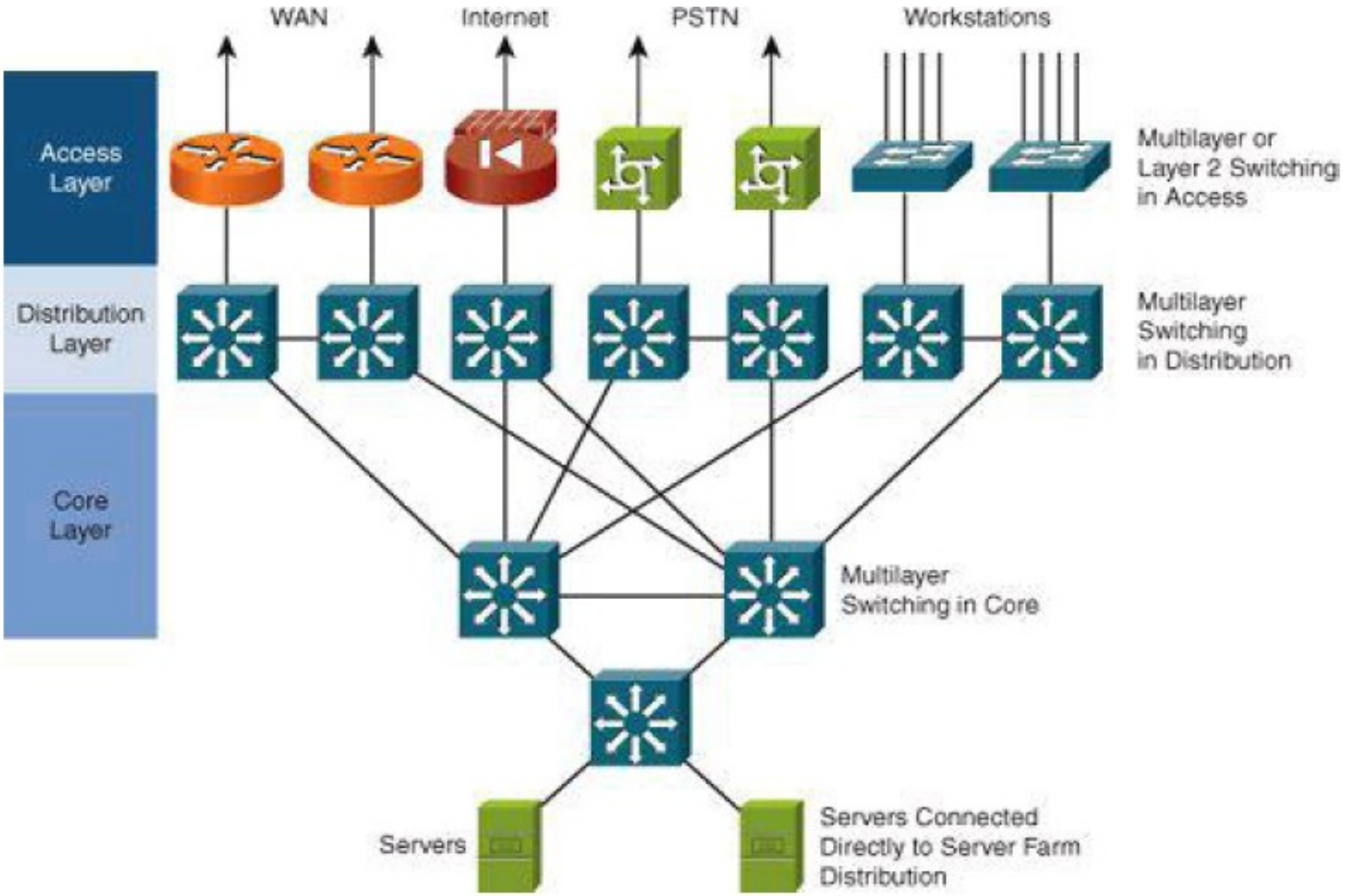


Hierarchical Network Model

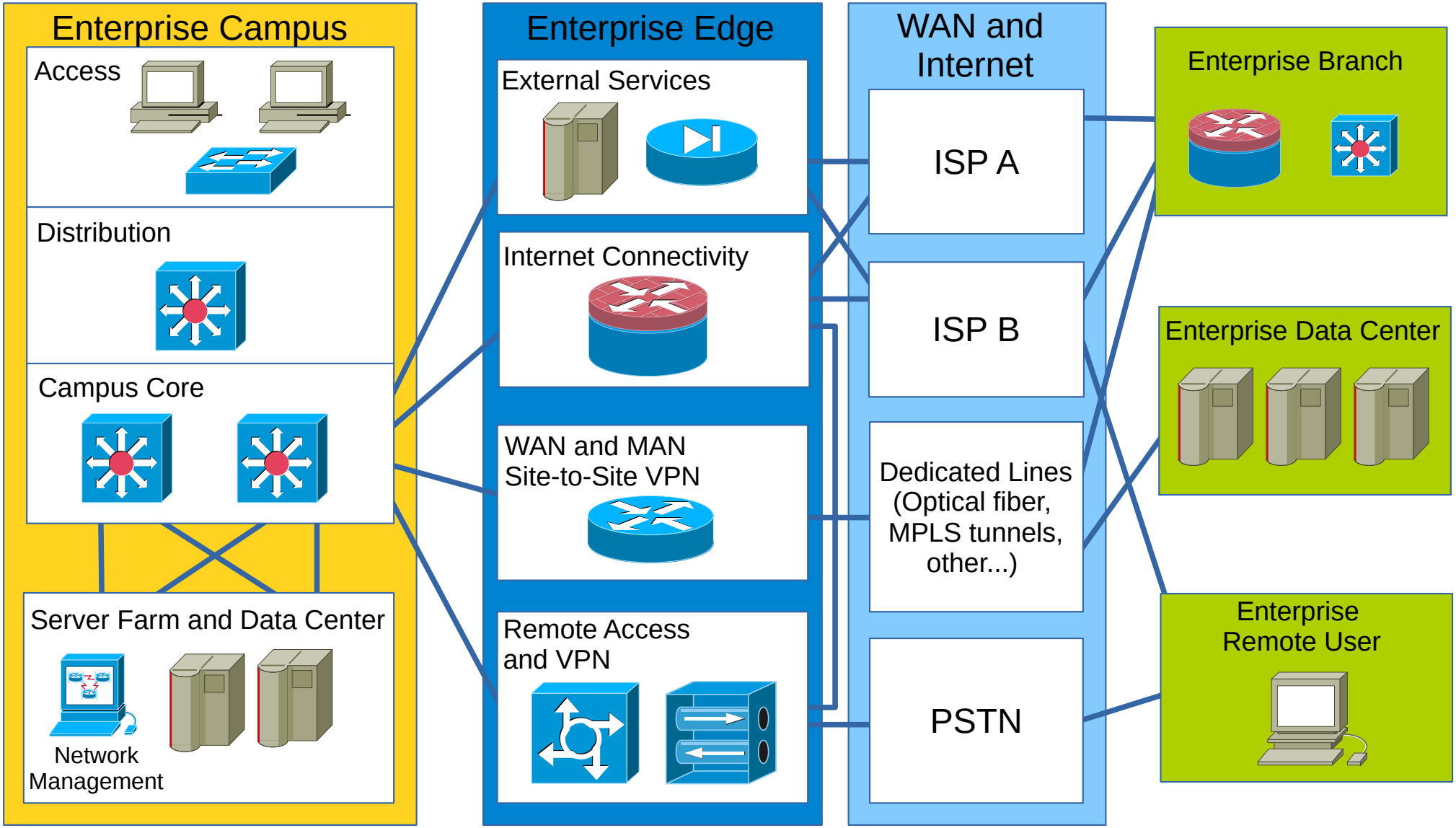


- Access layer
  - Provides user access to network.
  - Generally incorporates switched LAN devices that provide connectivity to workstations, IP phones, servers, and wireless access points.
  - For remote users or remote sites provide an entry to the network across WAN technology.
- Distribution layer
  - Aggregates LAN devices.
  - Segments work groups and isolate network problems.
  - Aggregates WAN connections at the edge of the campus and provides policy-based connectivity.
  - Implements QoS policies.
- Core layer
  - A high-speed backbone.
  - Core is critical for connectivity, must provide a high level of availability and adapt quickly to changes.
  - Should provide scalability and fast convergence.
  - Should provide an integration point for data center.

A Hierarchical Network



Modular Network Design



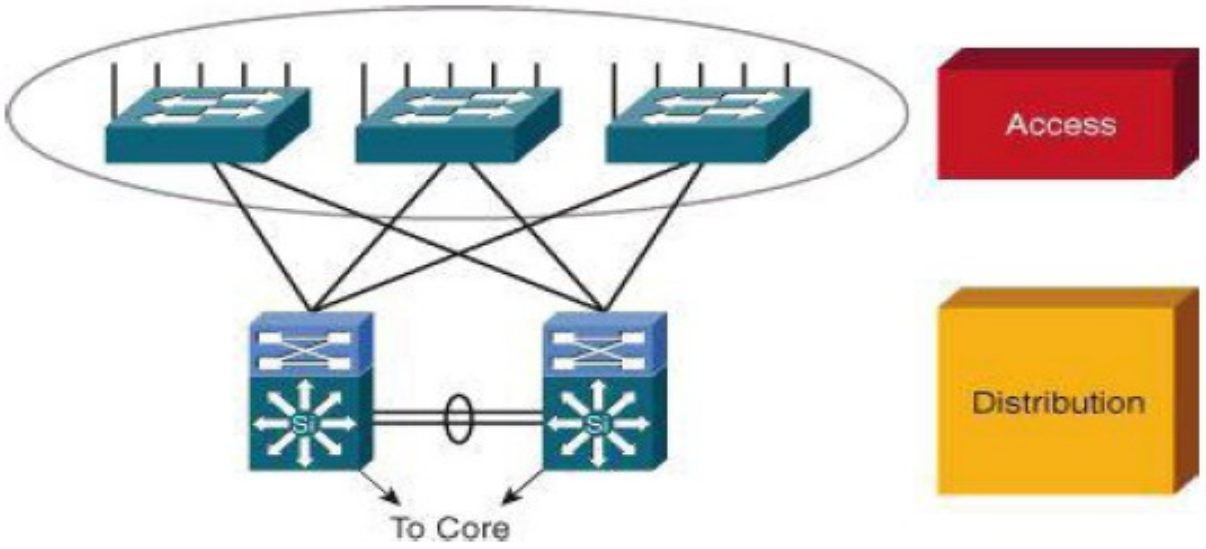
Network Modules (1)

- Campus
  - Operating center of an enterprise.
  - This module is where most users access the network.
  - Combines a core infrastructure of intelligent switching and routing with mobility, and advanced security.
- Data Center
  - Redundant data centers provide backup and application replication.
  - Network and devices offer server and application load balancing to maximize performance.
  - Allows the enterprise to scale without major changes to the infrastructure.
  - Can be located either at the campus as a server farm and/or at a remote facility.
- Branch
  - Allows enterprises to extend head-office applications and services to remote locations and users or to a small group of branches.
  - Provides secure access to voice, mission-critical data, and video applications.
  - Should provide a robust architecture with high levels of resilience for all the branch offices.

Network Modules (2)

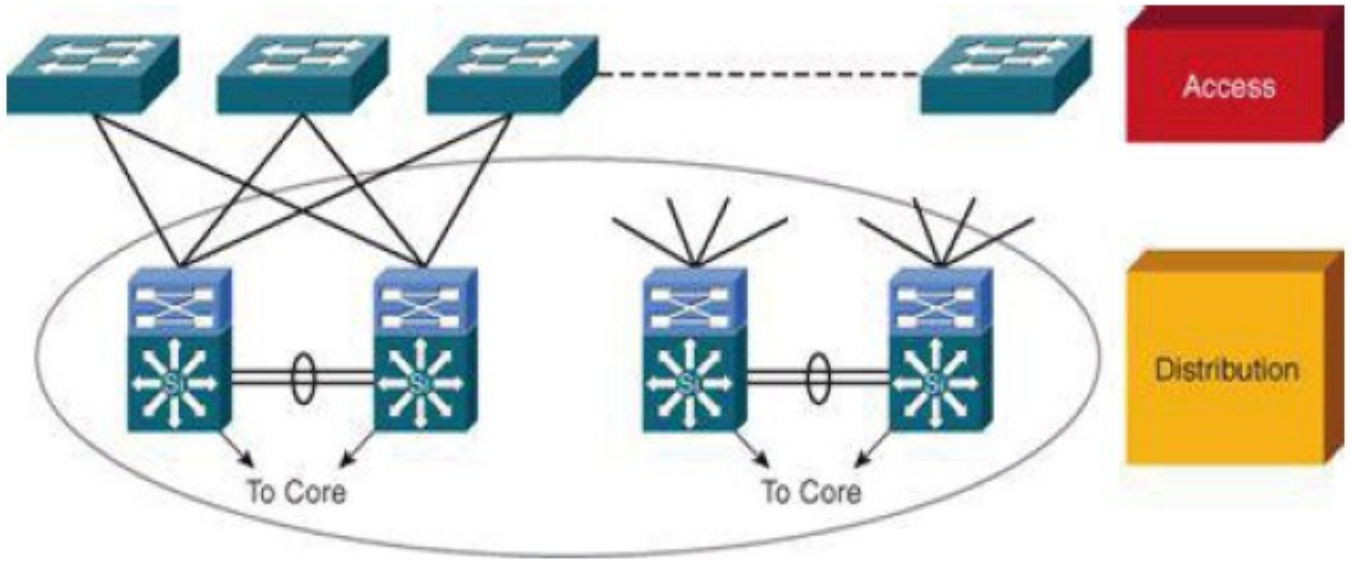
- WAN and MAN
  - Offers the convergence of voice, video, and data services.
  - Enables the enterprise a cost-effectively presence in large geographic areas.
  - QoS, granular service levels, and comprehensive encryption options help ensure the secure delivery to all sites.
  - Security is provided with multiservice VPNs (IPsec and MPLS) over Layer 2 or Layer 3 communications.
- Remote User
  - Allows enterprises to securely deliver voice and data services to a remote small office/home office (SOHO) over a standard broadband access service.
  - Allows a secure log in to the network over a VPN and access to authorized applications and services.

Designing the Access Layer



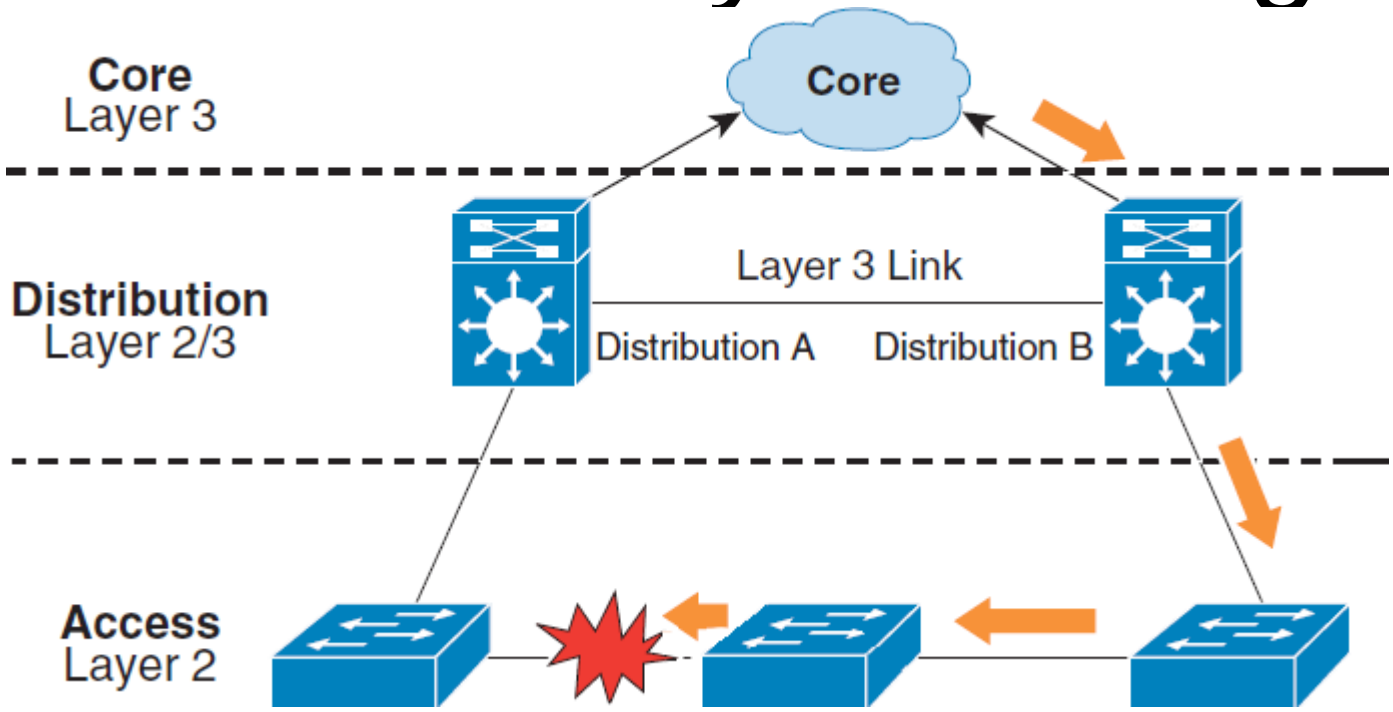
- High availability
  - Default gateway redundancy using multiple connections from access switches to redundant distribution layer switches.
  - Redundant power supplies.
- Other considerations
  - Convergence: the access layer should provide seamless convergence of voice into data network and providing roaming wireless LAN (WLAN).
  - Security: for additional security against unauthorized access to the network, the access layer should provide tools such as IEEE 802.1X, port security, DHCP snooping and dynamic ARP inspection (DAI).
  - Quality of service (QoS): The access layer should allow prioritization of critical network traffic using traffic classification and queuing as close to the ingress of the network as possible.
  - IP multicast: the access layer should support efficient network and bandwidth management using features such as Internet Group Management Protocol (IGMP) snooping.

Designing the Distribution Layer



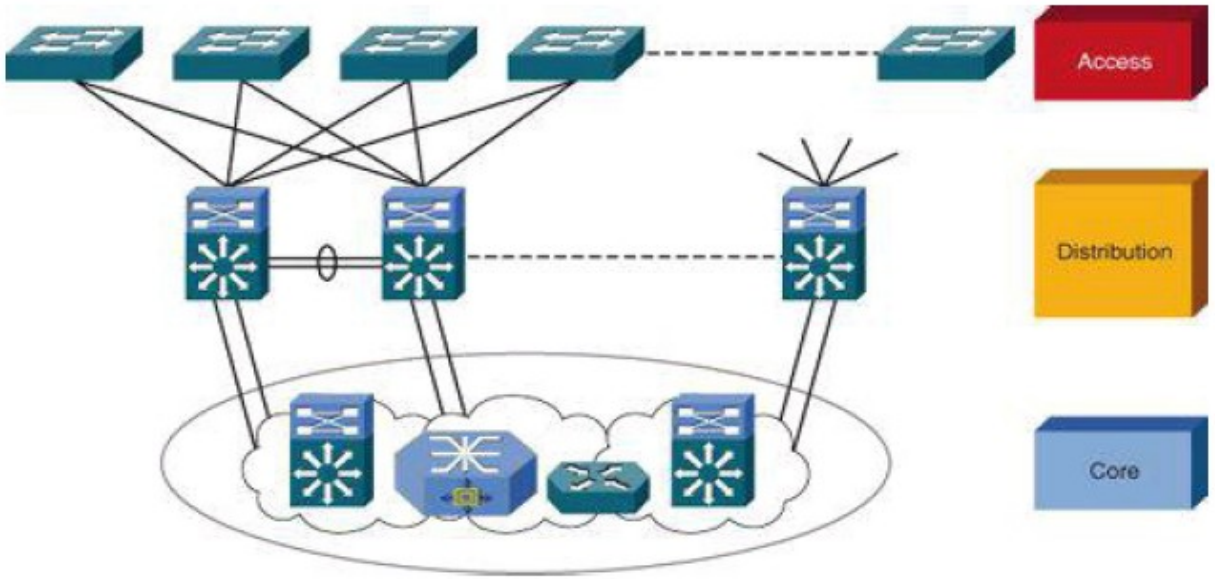
- Uses a combination of Layer 2 and multilayer switching to segment workgroups and isolate network problems, preventing them from impacting the core layer.
- Connects network services to the access layer and implements QoS, security, traffic loading balancing, and implements routing policies.
- Major design concerns: high availability, load balancing, QoS, and provisioning.
- In some networks, offers a default route to access layer routers and runs dynamic routing protocols when communicating with core routers.
- The distribution layer it is usually used to terminate VLANs from access layer switches.
- To further improve routing protocol performance, summarizes routes from the access layer.
- To implement policy-based connectivity, performs tasks such as controlled routing and filtering and QoS.

Avoid Daisy Chaining



- When using a L3 link between Distribution layer switches
  - In Access layer, any path from a switch should not require another switch from the Access layer.
  - In Distribution layer, any path between Distribution layer switches should not require a switch from the Access layer.
- When using a L2 link between Distribution layer switches
  - Daisy chain is acceptable, however
    - Could overload some Access layer switches.
    - Could increase STP convergence in case of failure.

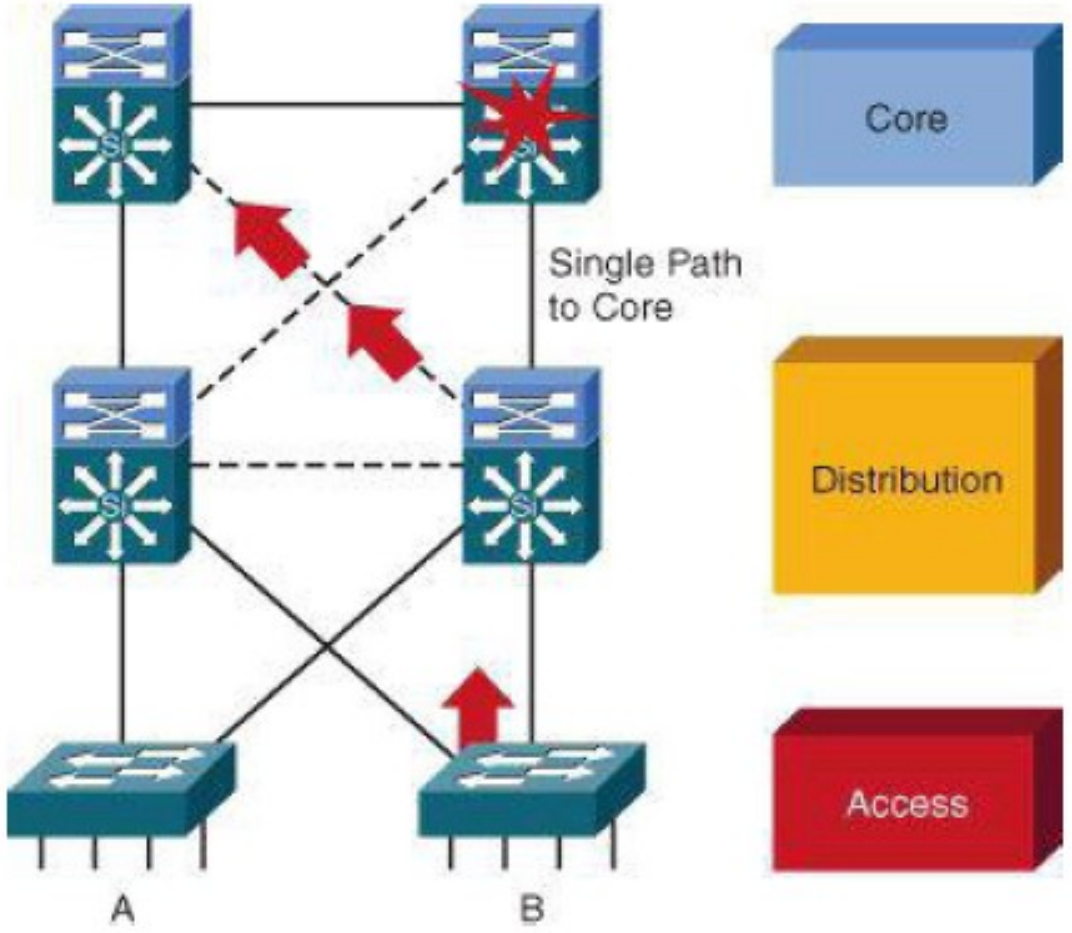
Designing the Core Layer



- Backbone for campus connectivity and is the aggregation point for the other layers.
- Should provide scalability, high availability, and fast convergence to the network.
  - The core layer should scale easily.
  - High-speed environment that should use hardware-acceleration, if possible.
  - The core should provide a high level of redundancy and adapt to changes quickly.
    - Core devices should be more reliable
    - Accommodate failures by rerouting traffic and respond quickly to changes in the network topology.
  - Implements scalable protocols and technologies.
  - Provides alternate paths and load balancing.
  - Packet manipulation should be avoided, such as checking access lists and filtering, which could slow down the switching of packets.
- Not all campus implementations require a campus core.
- The core and distribution layer functions can be combined at the distribution layer for a smaller campus.

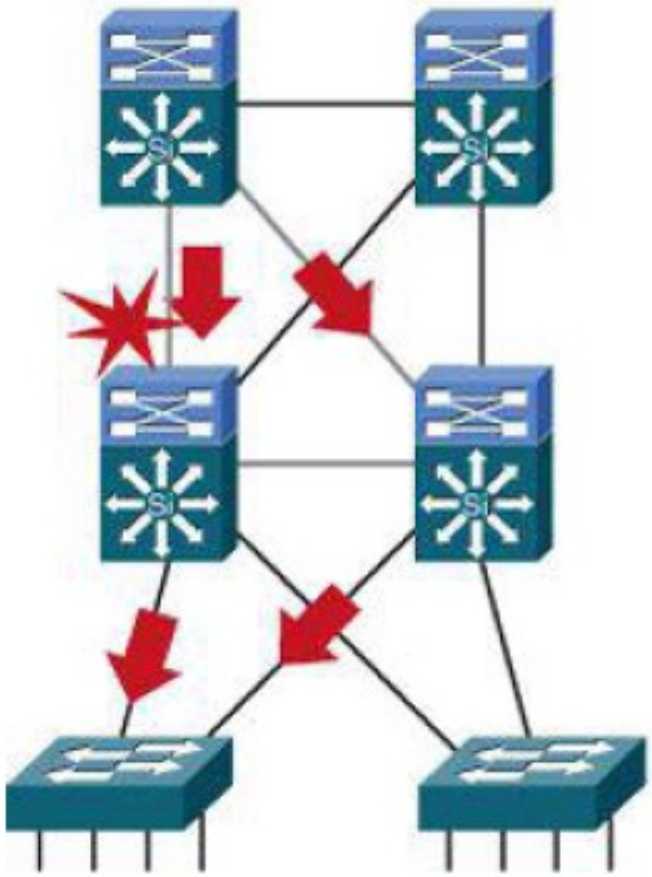
Provide Alternate Paths

- An additional link providing an alternate path to a second core switch from each distribution switch offers redundancy to support a single link or node failure.



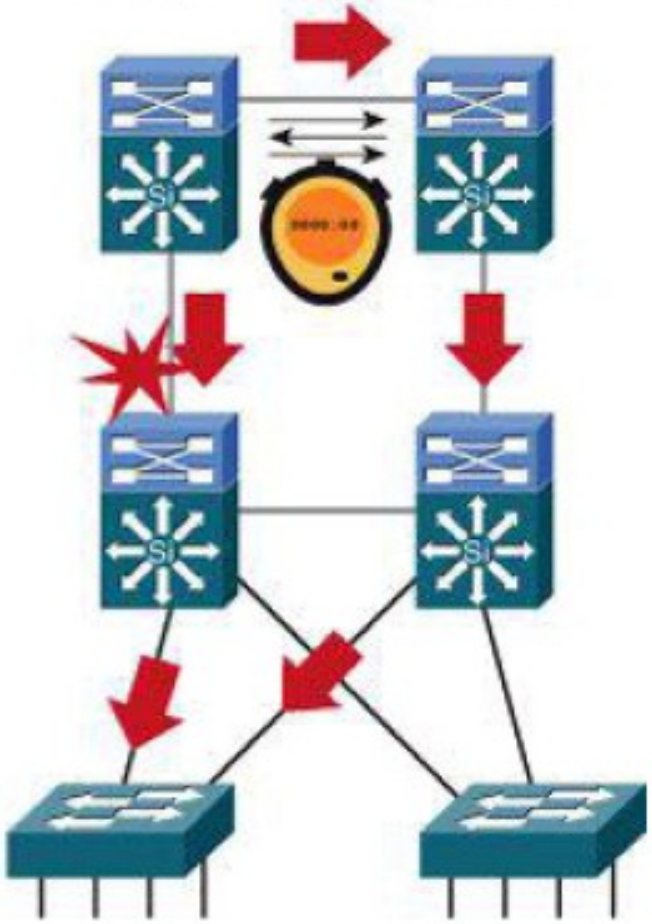
Core Redundant Triangles

Triangles: Link or box failure does *not* require routing protocol convergence.



Model A

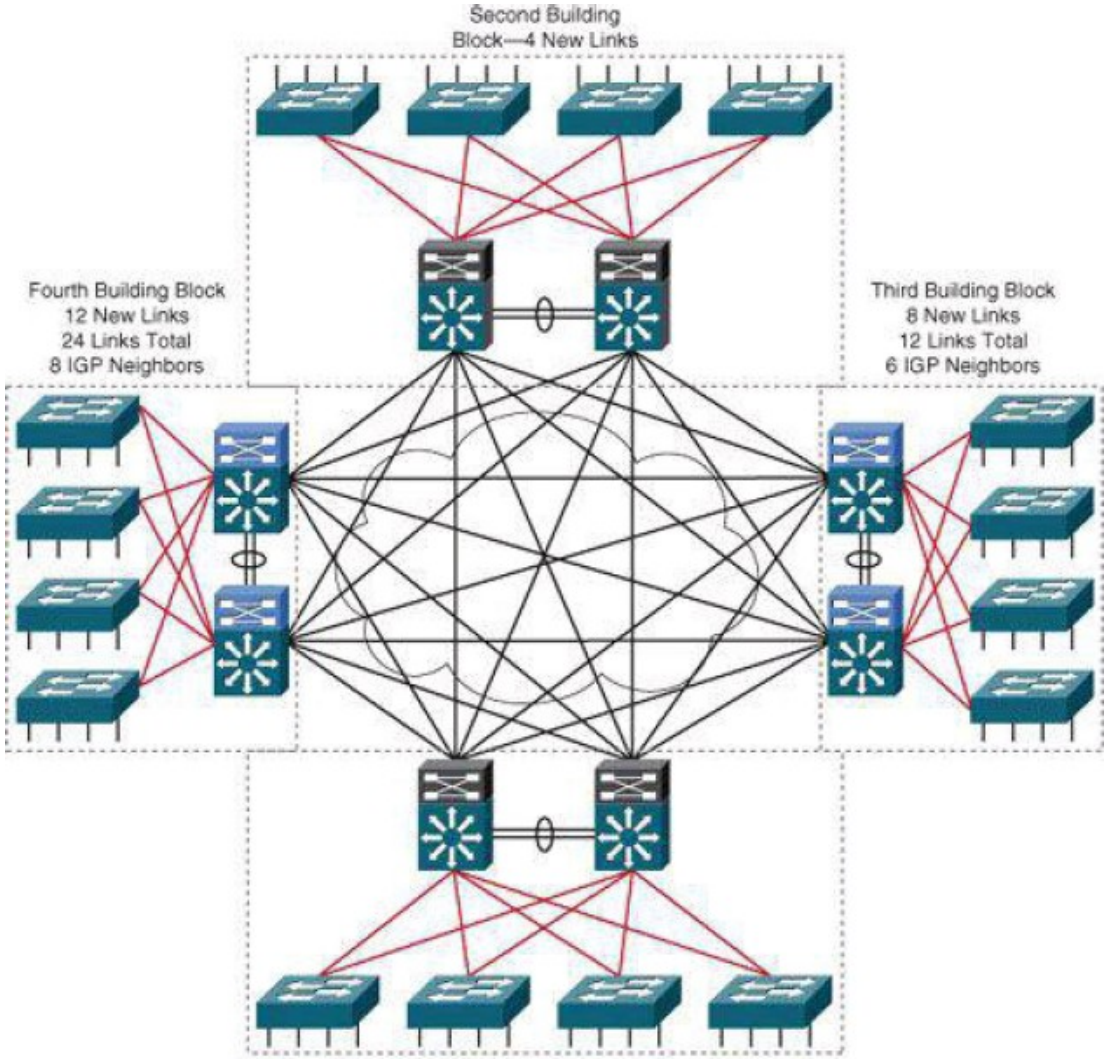
Squares: Link or box failure requires routing protocol convergence.



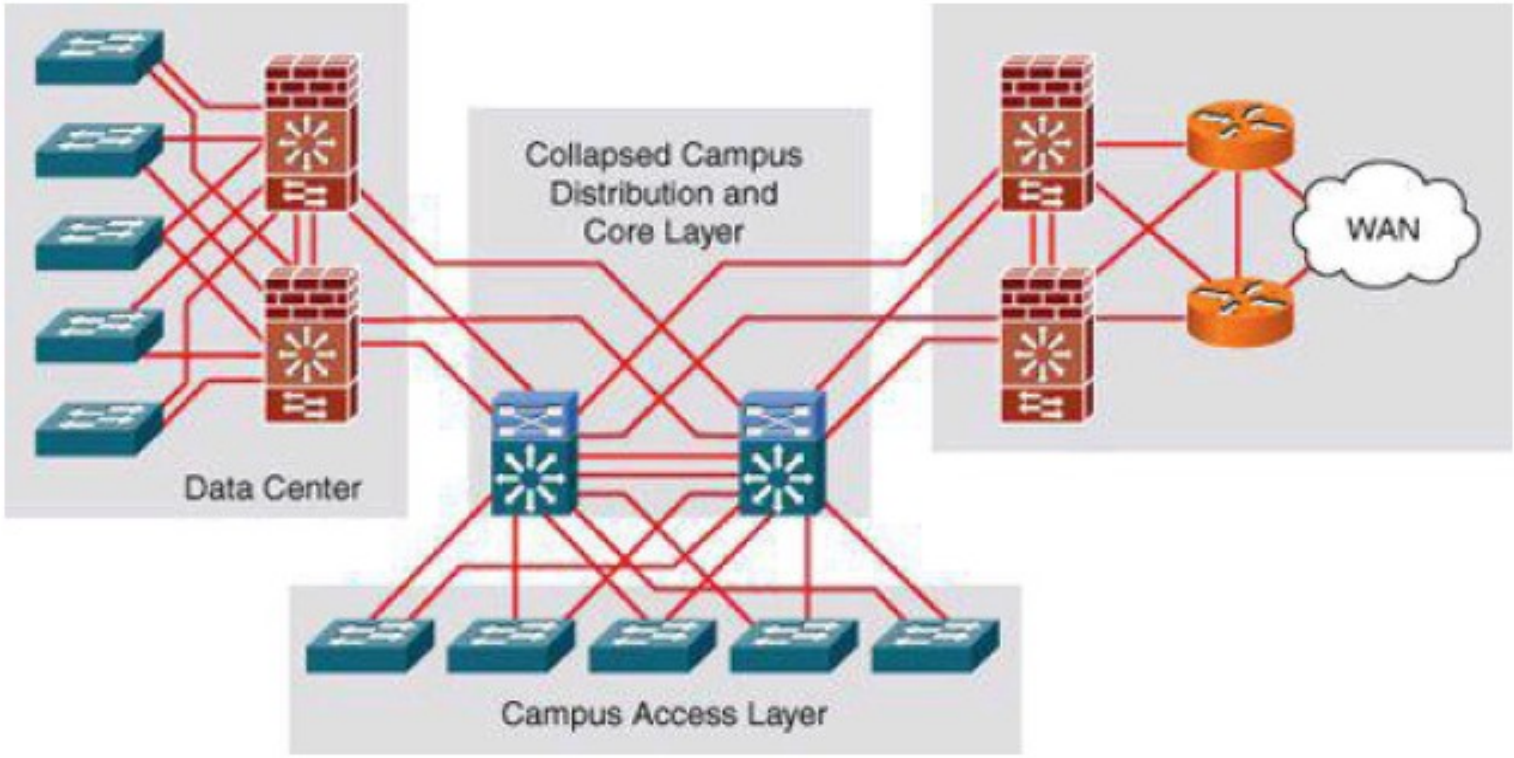
Model B

Without a Core Layer

- The distribution layer switches need to be fully meshed.
- Can be difficult to scale.
- Increases the cabling requirements.
- Routing complexity of a full-mesh design increases as new neighbors are added.
- Can be used in small campus with no perspective of growing.

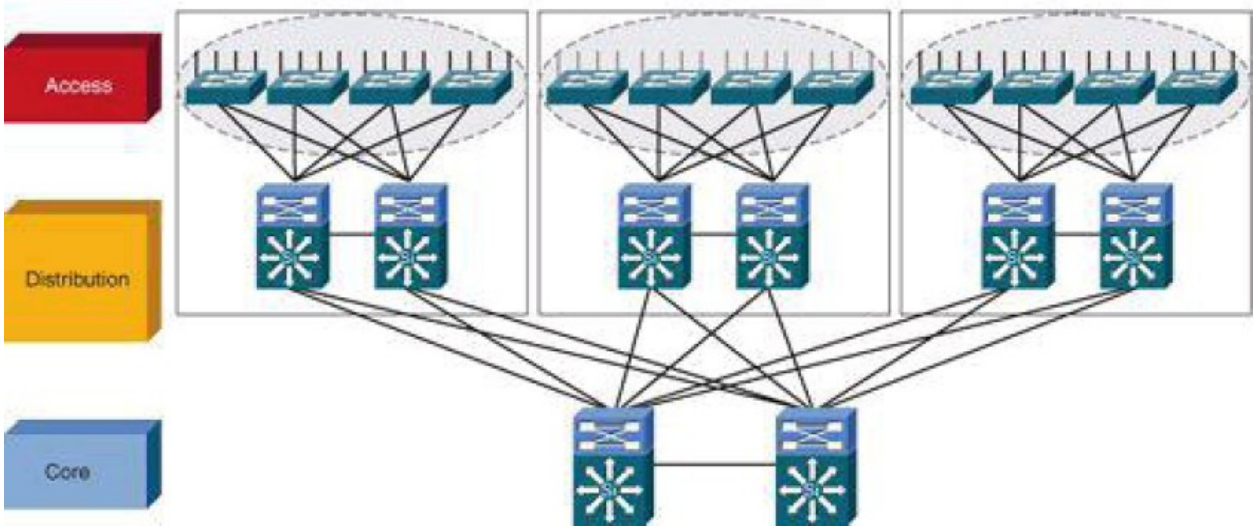


Collapsed Core Layer Architecture



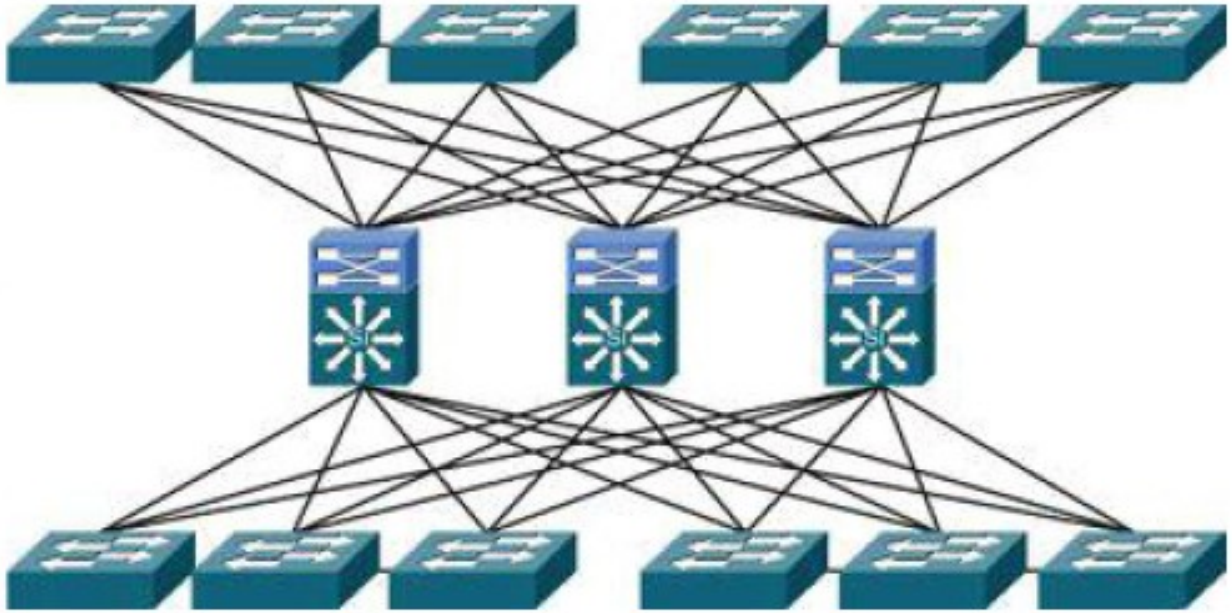
- In smaller networks, the core and the distribution layer can be only one,
  - Eliminates the need for extra switching hardware and simplifies the network implementation.
- However, eliminates the advantages of the multilayer architecture, specifically fault isolation.

Avoid Single Points of Failure



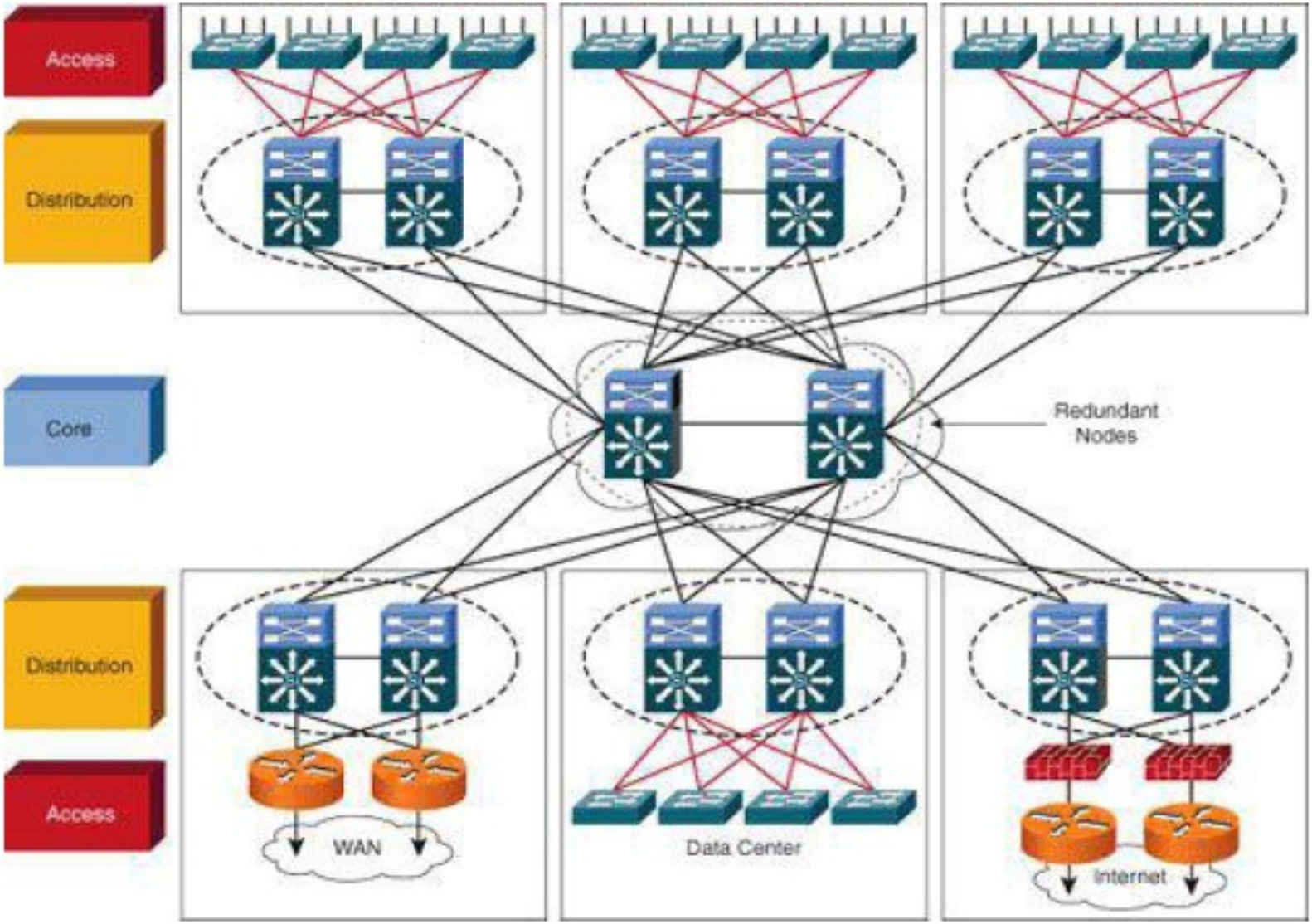
- With an hierarchical design,
  - In Distribution and Core Layers the single points of failure are easy to avoid with redundant links.
    - Don't forget redundant power and cooling!
  - In Access Layer, all L2 switches are single points of failure (only) to the user connected to them,
    - Solution 1, redundant backup hardware activated by a (proprietary) supervision mechanism to “replace” faulty equipment.
      - Copies full configuration and state to backup hardware.
    - Solution 2, have multiple connections between each user terminal and different access switches
      - Requires multiple network cards in user terminals and more plugs/wiring.
      - Cheaper?

Avoid Too Much Redundancy



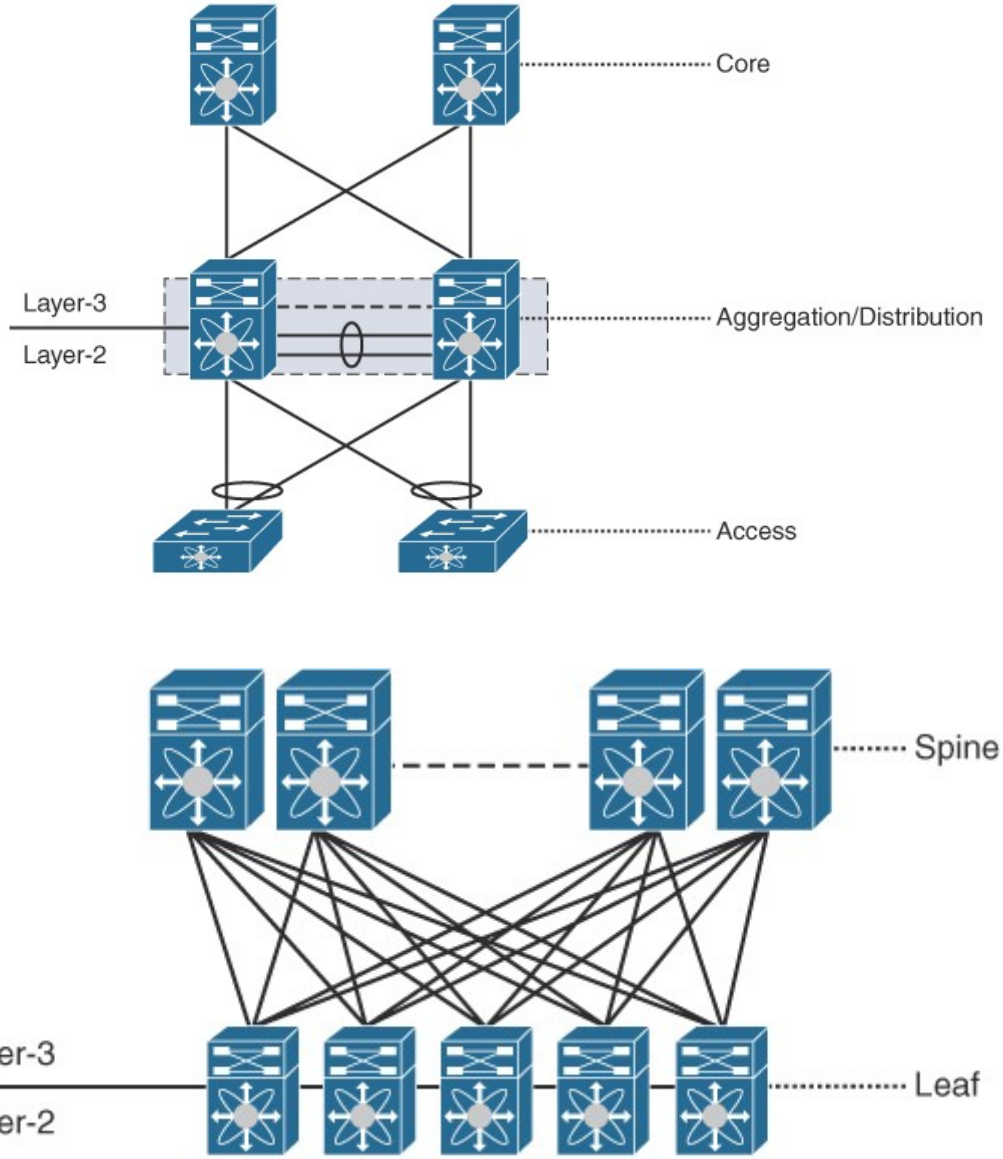
- Increases,
  - Routing complexity
  - Number of ports used
  - Wiring

Optimal Redundancy



Datacenter CLOS Topology

- With large-scale data center deployments, three-tier topologies have become scale bottlenecks.
- The classic three-tier topology evolved to a CLOS topology.
  - Original designed by Charles Clos in 1950 to find a more efficient way to handle telephonic call transfers.
- Eliminating the need for STP the network evolved to greater stability and scalability.
- Layer 3 moves to the Access Layer.
- Usually called Spine-and-Leaf Architecture.

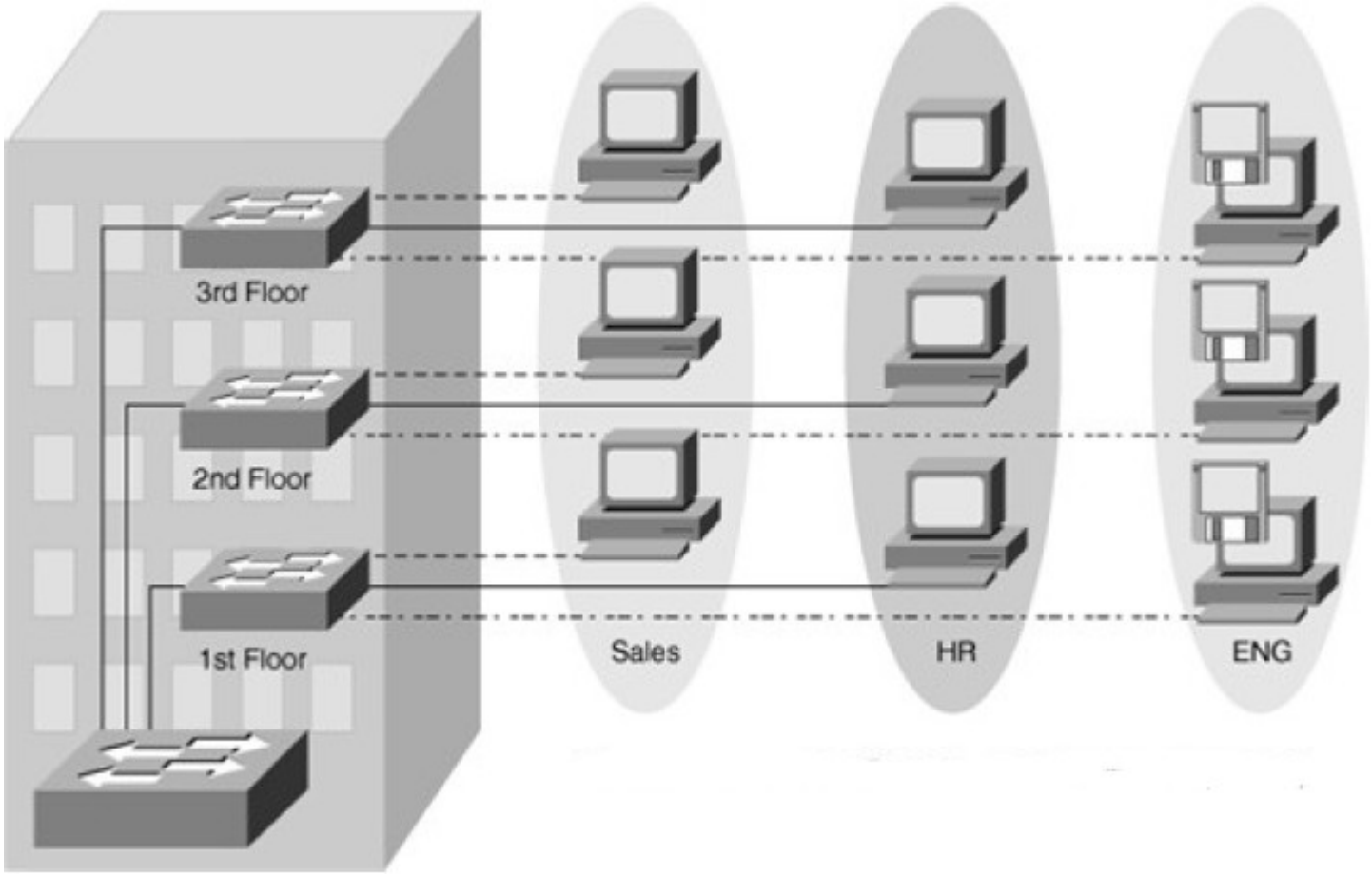


Virtual LANs

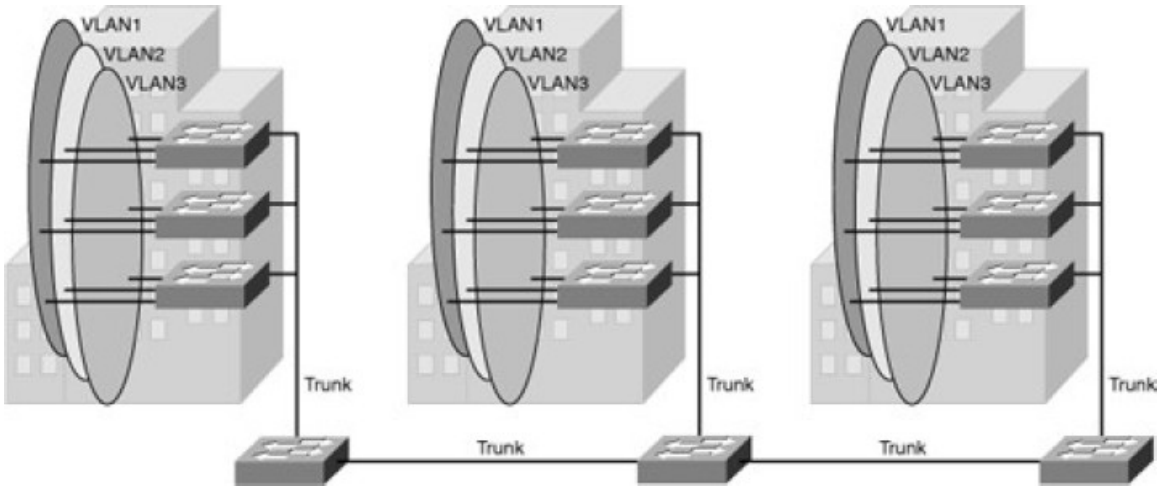
- Group of individual switch ports into switched logical *workgroup*
  - Restrict the broadcast domain to designated VLAN member ports
  - Communication between VLANs requires a router.
- Solves the scalability problems of large flat networks
  - By breaking a single broadcast domain into several smaller broadcast domains.

Implementing VLANs

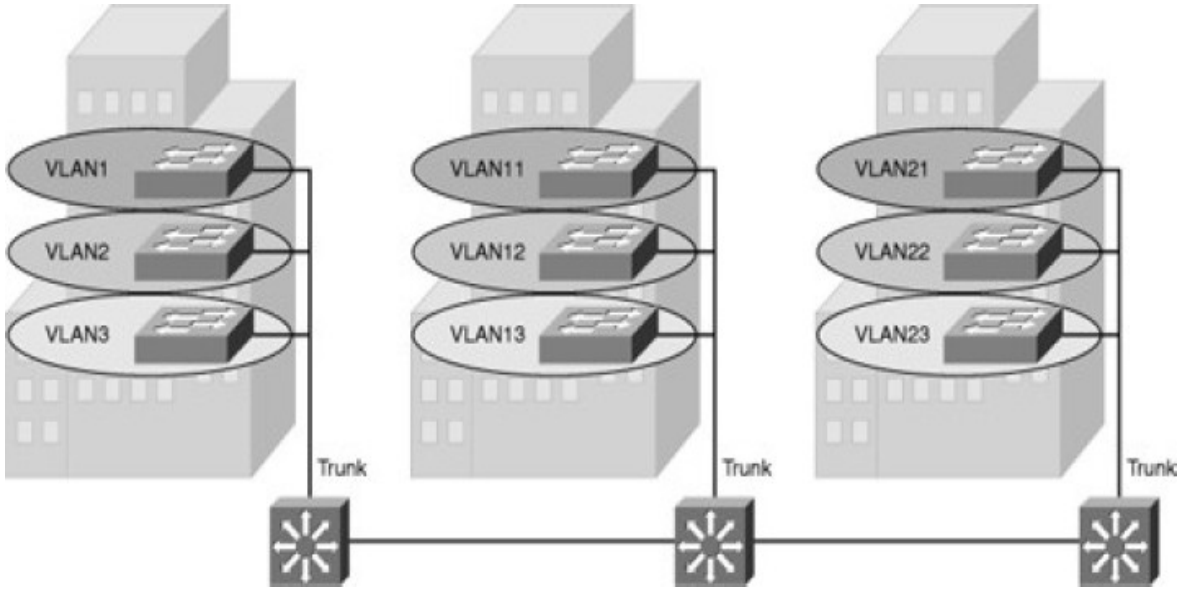
- VLAN is a logical group of end devices with a common set of requirements independent of their physical location.



VLAN Segmentation Models



- End-to-End VLAN
  - VLAN are associated with switch ports widely dispersed over the network



- Local VLAN
  - Local VLANs are generally confined to a wiring closet.

VLAN Segmentation (examples)

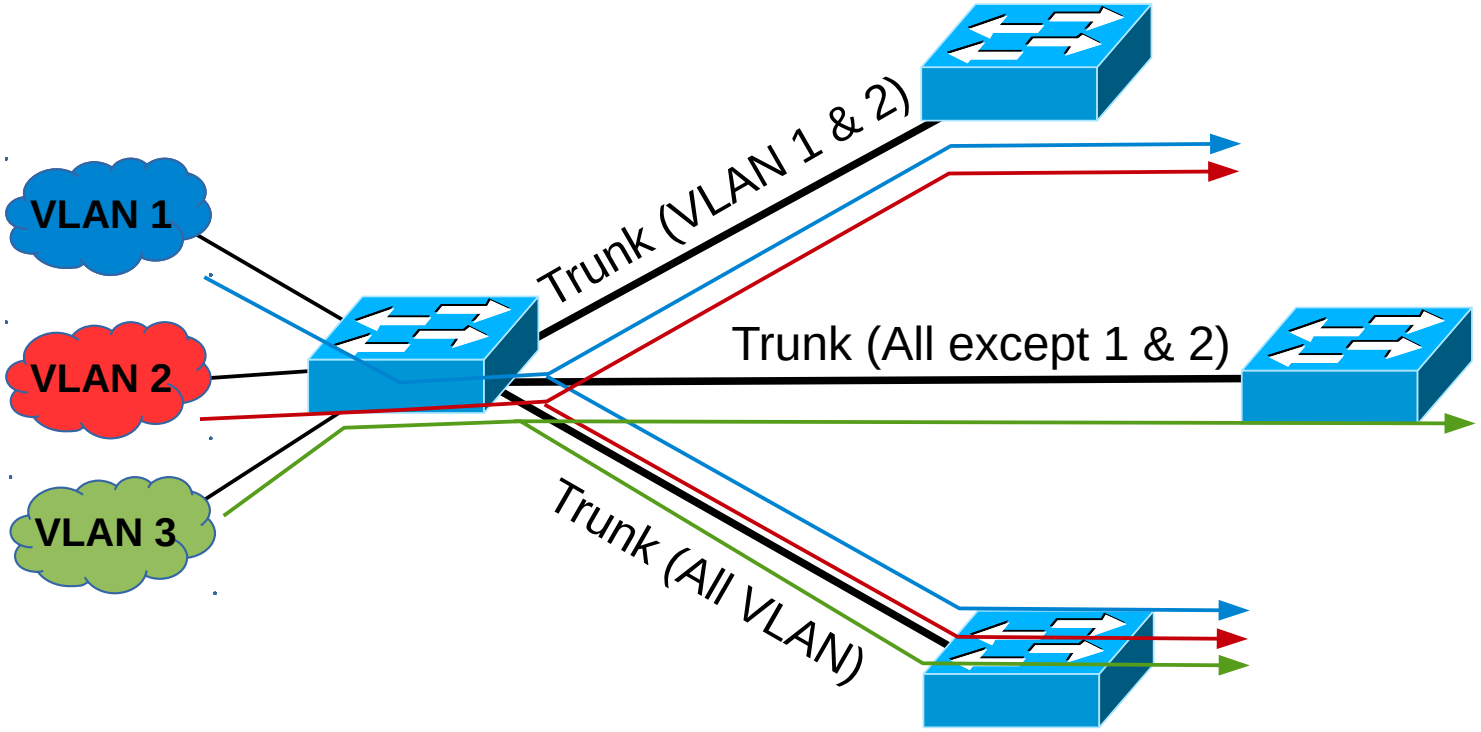
- Local VLANs
  - Per service/function
    - VoIP phones, Video conference, printers, cameras, PCs, servers, …
  - Per user role
    - Engineers I, engineers II, technicians, administrators, …
  - Per location
    - Building I, floor 4, right wing, etc...
  - Mixture of service/function, role, location
    - e.g.: VLAN of VoIP phones, of the Engineers in Building I.
- End-to-end VLANs
  - Services/roles that have a global scope within the network.
  - Wireless network
    - Same IP network (same IP address) independently of location.
    - To avoid IP changes when moving from location to location.
  - Administration VLAN (optional)
    - VLAN used by the network administrator to remotely access network equipments.
    - Same administrator of (all) equipments independent of location.

VLAN Segmentation Purpose

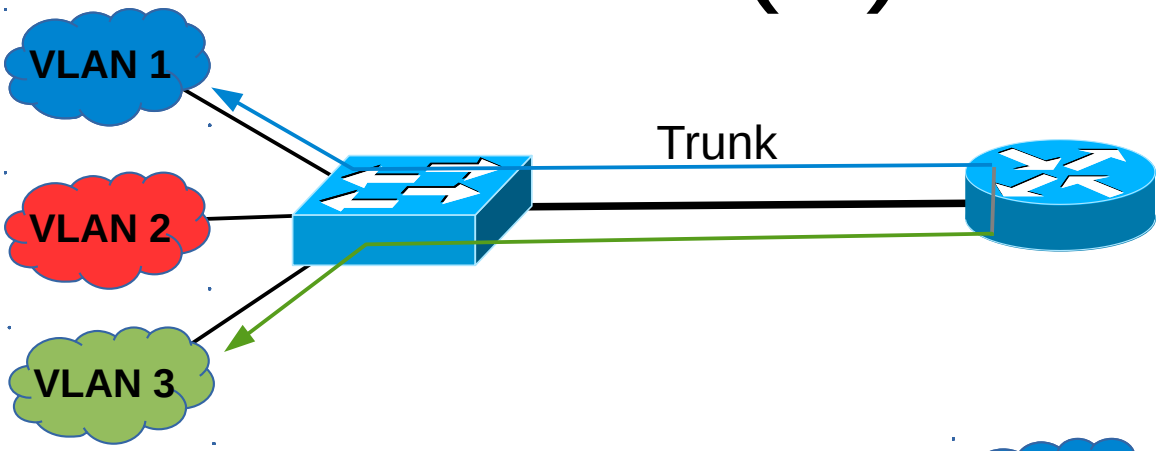
- Joint in the same logical network services/terminals/users with same traffic/security/QoS policies.
  - Each VLAN must have an unique IP (sub-)network.
  - May have more than one IP (sub-)network.
    - Including IPv4 public and IPv4 private networks.
    - And, IPv6 networks.
- Neighbor (local) VLANs with similar traffic/security/QoS policies should have IP (sub-)networks that can be summarized/aggregated.
  - E.g.: VLAN of VoIP phones in Building 1 (VLAN 21: 200.0.0.0/24)
  - VLAN of VoIP phones in Building 2 (VLAN 22: 200.0.1.0/24)
  - Summarized/aggregated address of VLAN21+VLAN22: 200.0.0.0/23.

Trunk Links

- A VLAN trunk carries traffic for multiple VLANs by using IEEE 802.1Q.
  - Inter-Switch Link (ISL) encapsulation is an alternative but it getting obsolete.
- Trunks may transport all VLAN or only some!

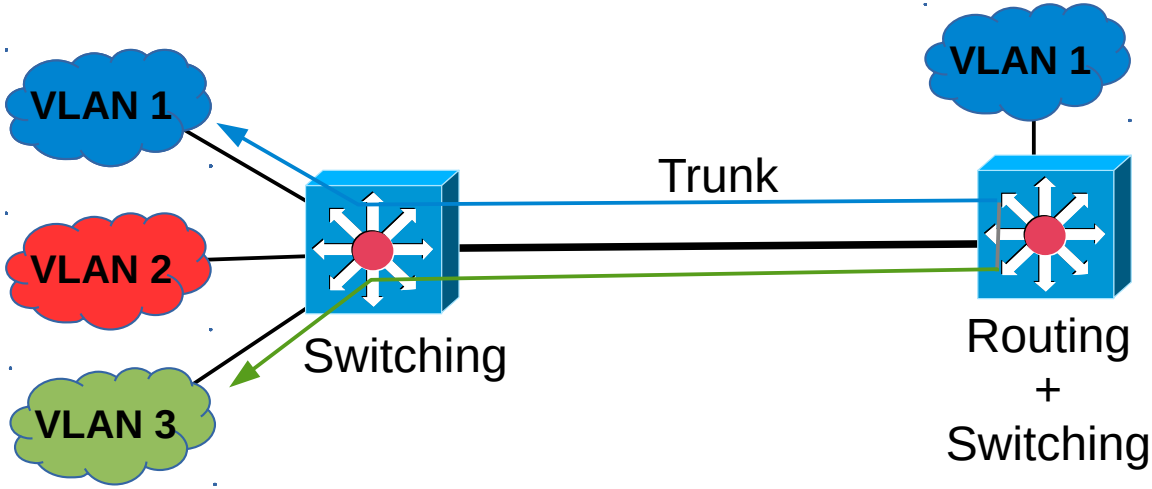


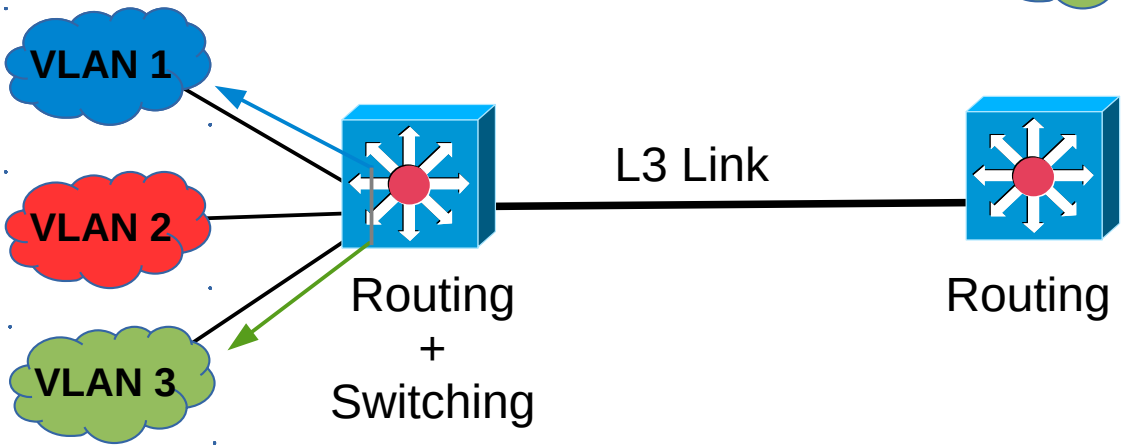
Inter-(V)LAN Routing



- L2 Switch + Router
  - Does not allow end-to-end VLANs.

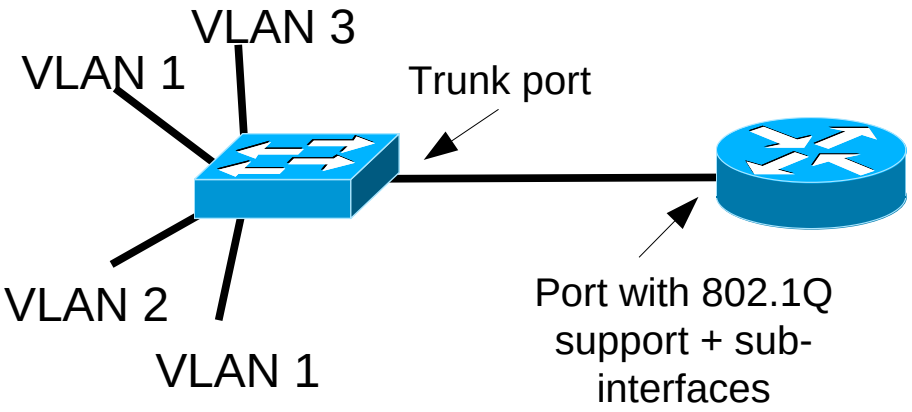
- L3 Switch + L3 Switch
  - Traffic between VLANs must “travel” until the first L3 Switch performing Routing.

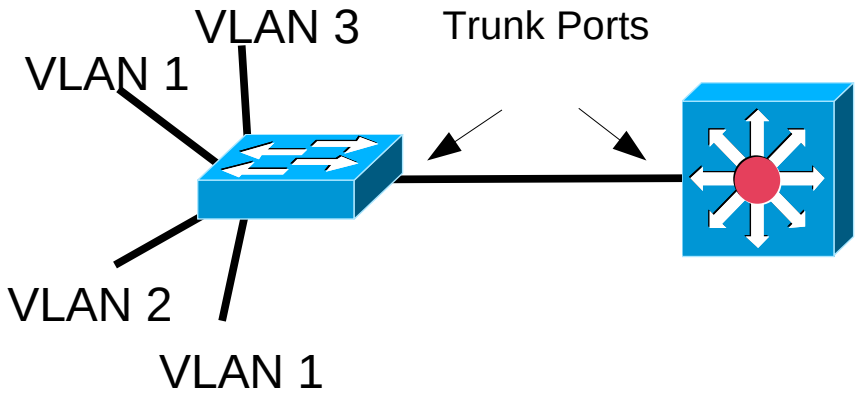




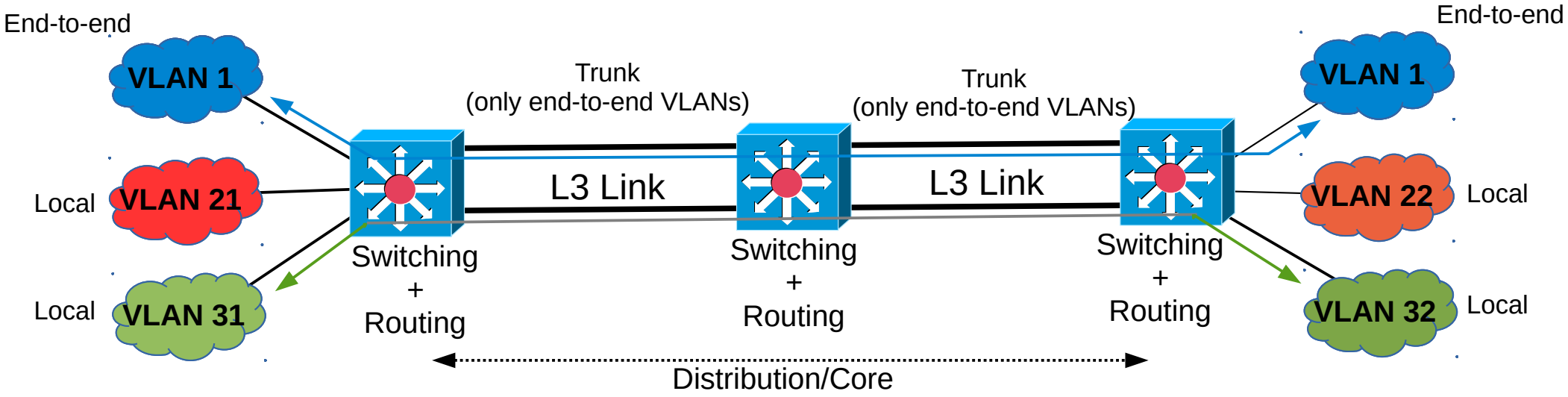
IP Connection between VLANs

- To communicate between different VLAN it is required to use Layer 3 (IP Routing).
- Common solutions:
  - A router with support to 802.1Q,
    - Connecting the physical router interface to a Trunk port.
    - The router's physical interface is sub-divided in sub-interfaces (one for each VLAN).
    - The IP gateway for a VLAN host is the IP address of the respective sub-interface in the Router.
  - A Layer 3 switch,
    - Connecting both switches (L3 and L2) using Trunk ports.
    - Each VLAN is mapped to a virtual Layer 3 interface.
    - The IP gateway for a VLAN host is the IP address of the respective virtual interface in the L3 switch.





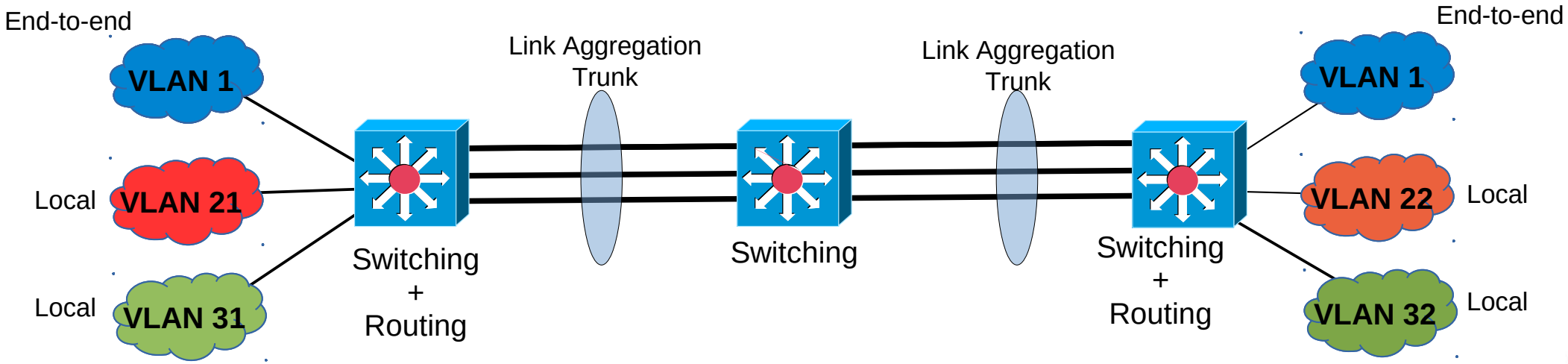
Inter-(V)LAN Traffic (1)



- End-to-end VLANs traffic **should be switched** over the Distribution/Core layers
  - Using a trunk (for end-to-end VLANs only).
- Local VLANs traffic **should be routed** over the Distribution/Core layers
  - Using standard layer 3 Links.
  - Using static routing (not the best solution!).
  - Exchange the routing information only through the L3 links
    - End-to-end VLAN should be passive interfaces for the routing processes.
      - Routes are not exchanged → Traffic is not routed!

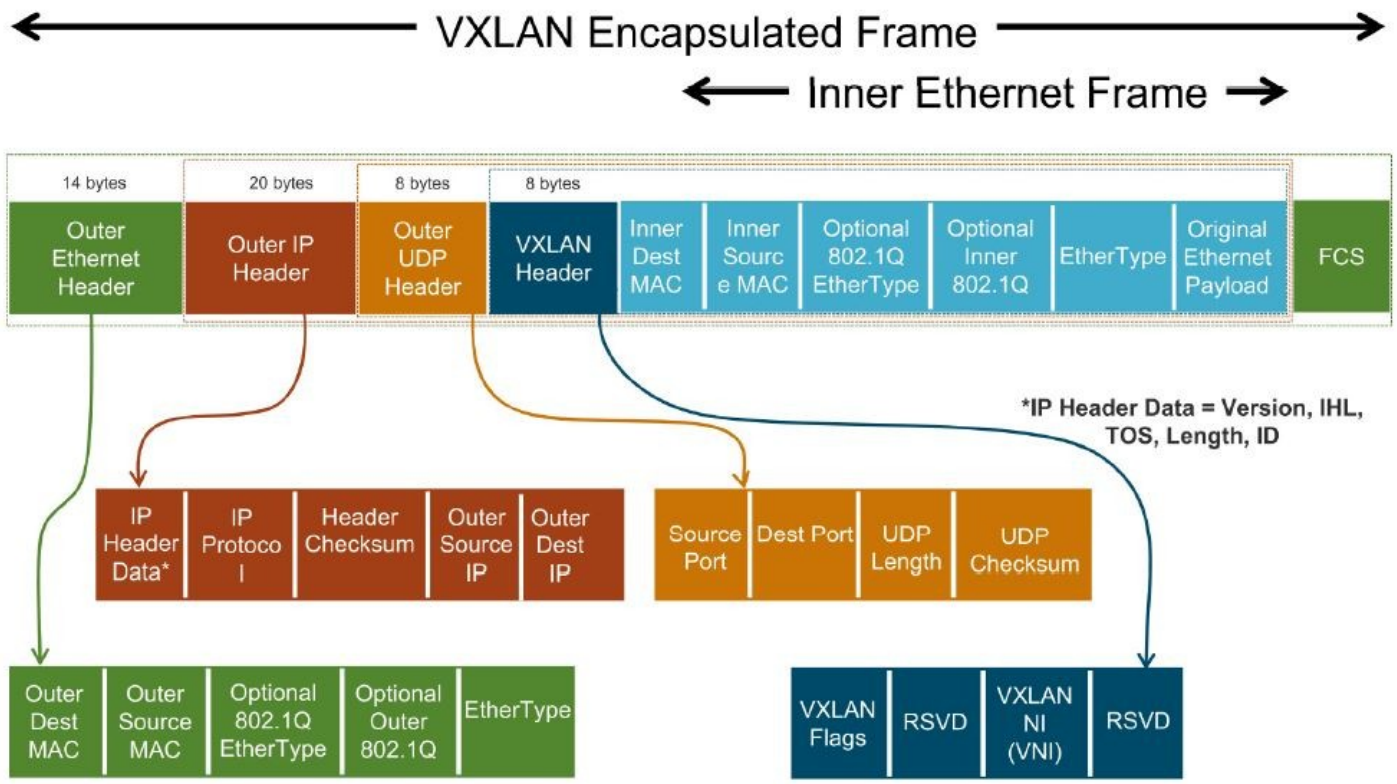
Ethernet Link Aggregation

- The throughput/speed of one connection link may not be enough to fulfill the requirements.
- Multiple Ethernet links may aggregated, provide a seamless trunk connection with N times the single throughput/speed of one link.
- Ethernet frames are “load-balanced” between all available physical links.



Virtual Extensible LAN (VXLAN)

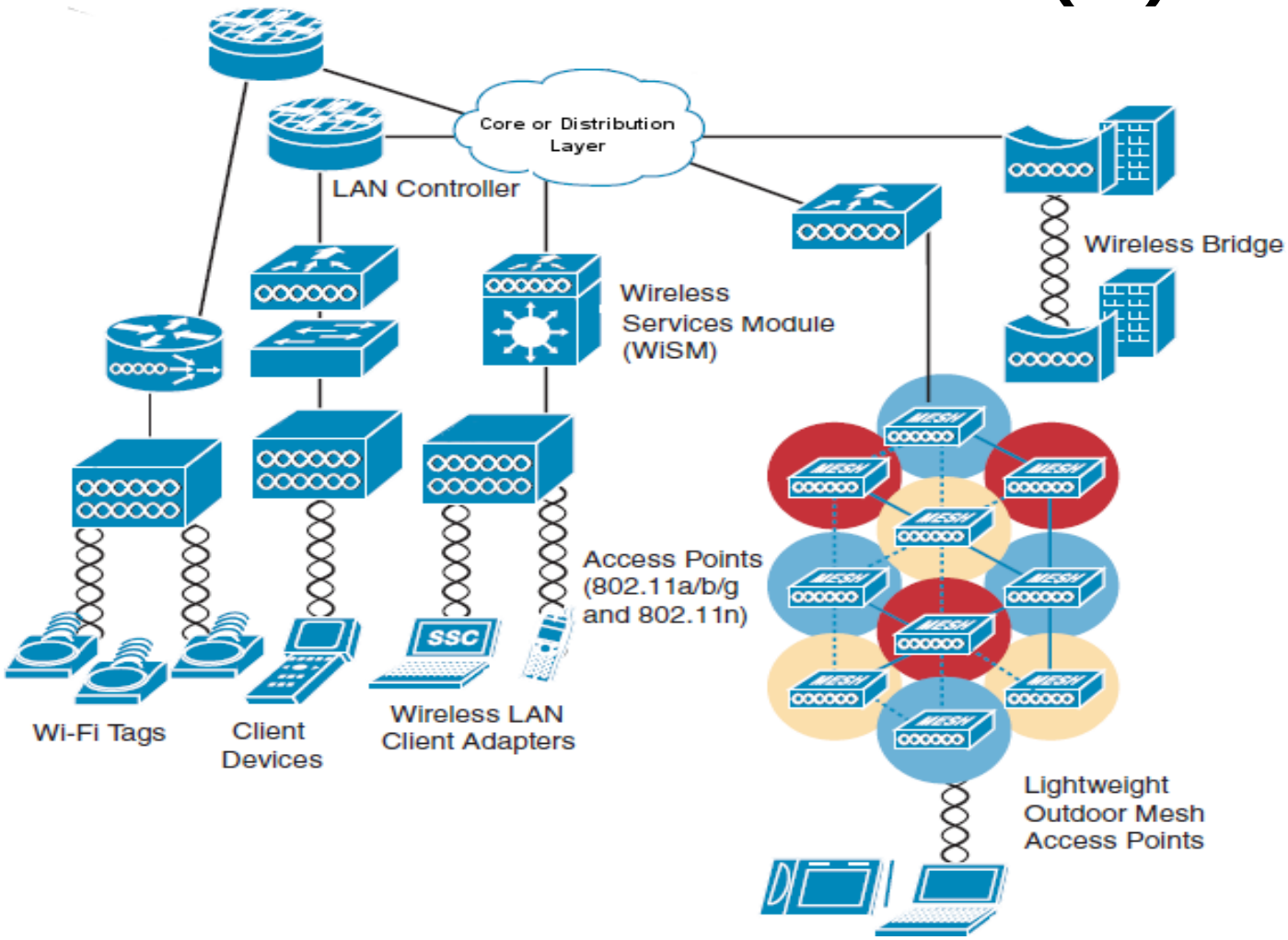
- Encapsulates OSI Layer 2 Ethernet frames within Layer 4 UDP datagrams.
  - Default port 4789.
- Alternative to 802.1Q.



Spanning Tree Protocol

- STP enables the network to deterministically block interfaces and provide a loop-free topology in a network with redundant links.
- There are several STP Standards and Features:
  - STP is the original IEEE 802.1D version (802.1D-1998) that provides a loop-free topology in a network with redundant links.
  - RSTP, or IEEE 802.1W, is an evolution of STP that provides faster convergence of STP.
  - Multiple Spanning Tree (MST) is an IEEE standard. MST maps multiple VLANs into the same spanning-tree instance.
  - Per VLAN Spanning Tree Plus (PVST+) is a Cisco enhancement of STP that provides a separate 802.1D spanning-tree instance for each VLAN configured in the network.
  - RPVST+ is a Cisco enhancement of RSTP that uses PVST+. It provides a separate instance of 802.1W per VLAN.
- Recommended Practices for STP
  - Define by configuration (using STP priority) the root bridge/switch.
  - Use the same cost in all interfaces (if possible).

Wireless Network(s)

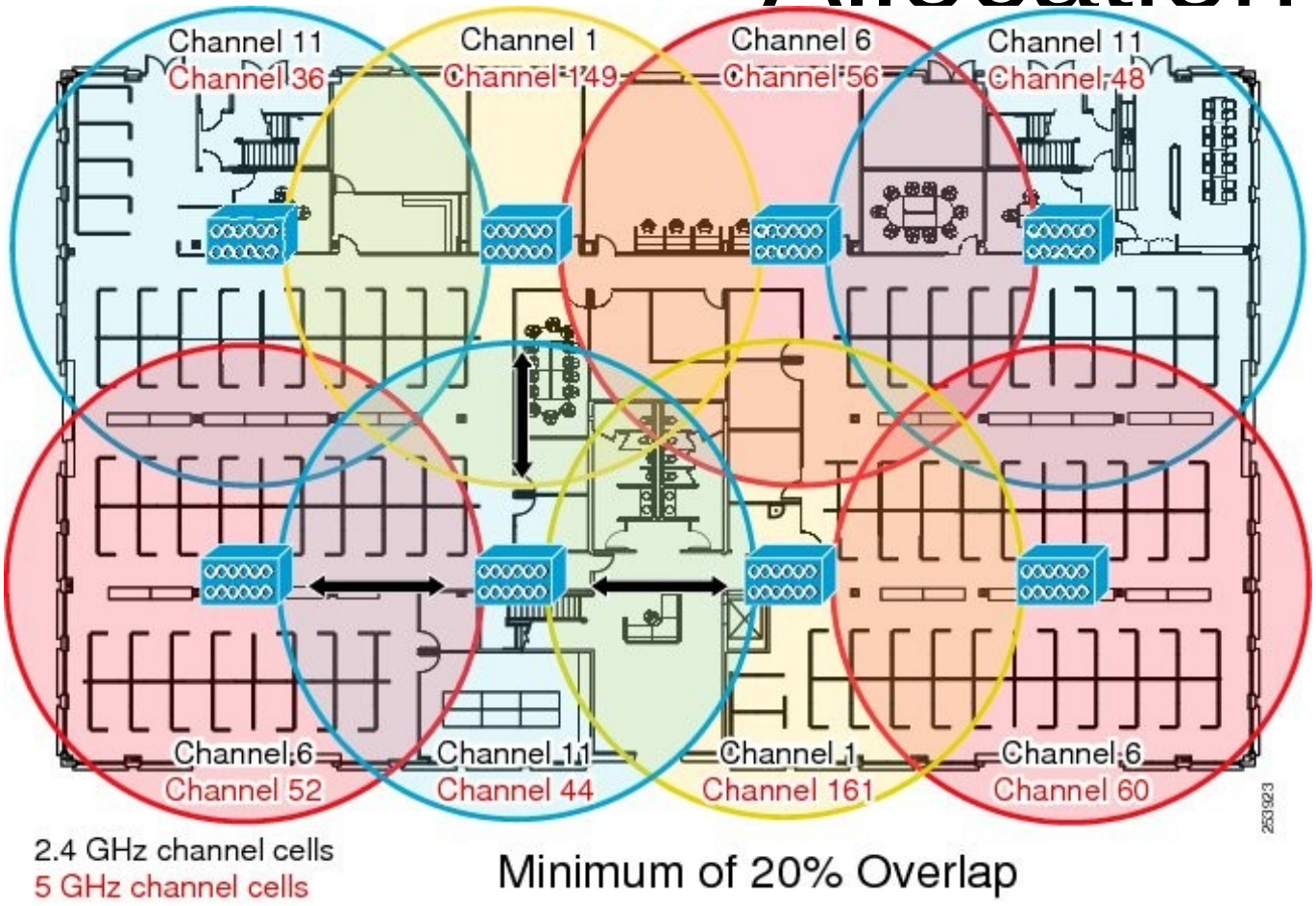


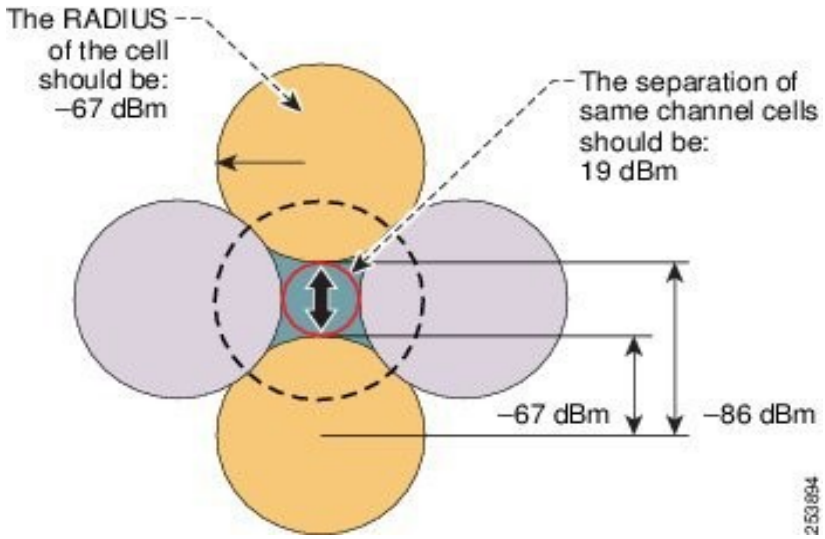
- Wireless networking technologies should have an integration point at core or distribution layers.
- In terms of network architecture a WLAN can be seem as any LAN.
  - Except that we have mobility and must have seamless roaming while moving.
- A large number of AP can be managed by a (Wireless) LAN Controller.

VLANs on Access Points

- AP have trunk ports to distribution/core switches.
- “Wired” VLANs must/can be extended to the wireless domain.
  - e.g., VLAN 30 “Green” and VLAN 10 “Red”.
- Each SSID can be mapped to a VLAN.
  - Different SSID/VLAN can have different security policies.
- Wireless VLANs should be configured as end-to-end.
  - Mobility and AP roaming should not break Layer 3 connectivity.
  - IP address should be the same → same VLAN with campus.
- A Native VLAN is required to provide management capability and client authentications.
  - Never extended to the wireless domain!!
    - e.g., VLAN 1.

AP Placement and Channel Allocation





- 802.11n or 802.11ac 5GHz deployment does not have the overlap or collision domain issues of 2.4GHz.

IP Routing Overview

- Routers forward packets toward destination networks.
- Routers must be aware of destination networks to be able to forward packets to them.
- A router knows about the networks directly attached to its interfaces
- For networks not directly connected to one of its interfaces, however, the router must rely on outside information.
- A router can be made aware of remote networks by:
  - **Static routing**: An administrator manually configure the information.
  - **Dynamic routing**: Learns from other routers.

  Policy based routing: Manually routing rules that outweigh static/dynamic routing and may depend on parameters other than the destination address.

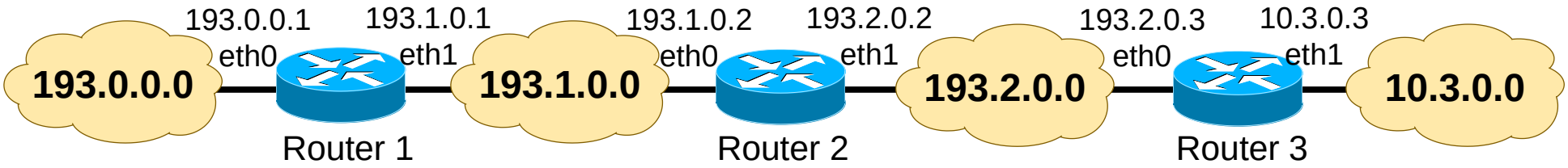
Default Routes

- In some circumstances, a router does not need to recognize the details of remote networks.
- The router can be configured to send all traffic (or all traffic for which there is not a more specific entry in the routing table) to a specific neighbor router.
- This is known as a default route.
- Default routes are either dynamically advertised using routing protocols or statically configured.
- IPv4 default route - 0.0.0.0/0
- IPv6 default route - ::/0

Static Routing

- Stating routing do not react to network topology changes.
  - If a link fails, the static route is no longer valid if it is configured to use that failed link, so a new static route must be configured.
  - Connectivity may be lost until intervention of an administrator.
- Static routing does not scale well when network grows.
  - Administrative burden to maintain routes may can become excessive.
- Static routes can be used in the following circumstances:
  - When the administrator needs total control over the routes used by the router.
  - When a backup to a dynamically recognized route is necessary.
  - When it is used to reach a network accessible by only one path (a stub network).
    - There is no backup link, so dynamic routing has no advantage.
  - When a router connects to its ISP and needs to have only a default route pointing toward the ISP router, rather than learning many routes from the ISP.
    - Again, a single path of access without backup.
  - When a router is underpowered and does not have the CPU or memory resources necessary to handle a dynamic routing protocol.
  - When it is undesirable to have dynamic routing updates forwarded across low bandwidth links.

Static Routing Examples



- Example 1
  - Router2 do not know networks 193.0.0.0/24 and 10.3.0.0/24
  - Necessary static routes:
    - 193.0.0.0/24 accessible through 193.1.0.1 (eth1, Router1)
    - 10.3.0.0/24 accessible through 193.2.0.3 (eth0,Router3)
- Example 2
  - Router1 do not know networks 193.2.0.0/24 and 10.3.0.0/24
  - Necessary static routes:
    - 193.2.0.0/24 accessible through 193.1.0.2 (eth0, Router2)
    - 10.3.0.0/24 accessible through 193.1.0.2 (eth0, Router2)

      OR
    - Using default route: 0.0.0.0/0 accessible through 193.1.0.2 (eth0, Router2)

Dynamic Routing

- Dynamic routing allows the network to adjust to changes in the topology automatically, without administrator involvement.
- Routers exchange information about the reachable networks and the state of each network/link.
  - Routers exchange information only with other routers running the same routing protocol.
  - When the network topology changes, the new information is dynamically propagated throughout the network, and each router updates its routing table to reflect the changes.

(Complex) Routing Tables

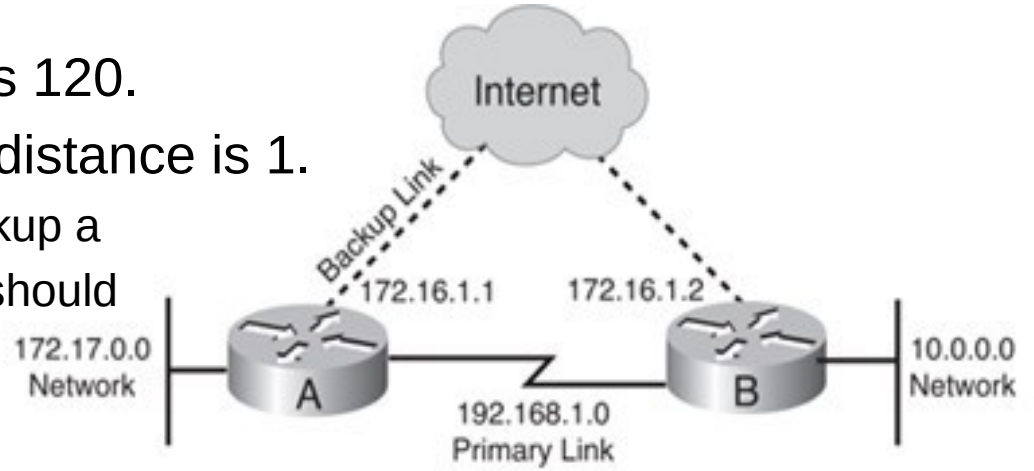
- An IP address may have multiple matches on a Routing Table:
  - Example: 192.168.1.12
  - Will match:
    - 192.168.1.0/25 via ...
    - 192.168.1.0/24 via ...
    - 192.168.0.0/23 via ...
    - 192.168.0.0/16 via ...
    - …
  - Router will choose entry with the largest network prefix (most specific network).
    - i.e., 192.168.1.0/25 via ...
- Load balancing
  - Routing tables may have more than one path for each network
    - Traffic will be divided by all entries.
    - By packet, flow (TCP session, UDP IPs/port), etc...
      - E.g, packet 1 path 1, packet 2 path 2, packet 3 path 1, …
      - Flow 1 path 1, flow 2 path 2, flow 3 path 3, flow 4 path 1, flow 5 path 2, ...

Administrative Distance

- Most routing protocols have metric structures and algorithms that are incompatible with other protocols.
- It is critical that a network using multiple routing protocols be able to seamlessly exchange route information and be able to select the best path across multiple protocols.
- Routers use a value called administrative distance to select the best path when they learn from different routing protocols the same destination (same network prefix and mask length).
- The Protocol/Method with the lowest Administrative Distance is preferred
  - The Administrative Distance value is configurable.
- Example:
  - Static [**1**/1] 192.168.1.0/24 via … ← Chosen!
  - RIP [**120**/1] 192.168.1.0/24 via …
  - OSPF [**110**/1] 192.168.1.0/24 via ...

Floating Static Routes

- Based on the default administrative distances, routers use static routes over any dynamically learned route.
  - However, this default behavior might not be the desired behavior.
  - For example, when you configure a static route as a backup to a dynamically learned route, you do not want the static route to be used as long as the dynamic route is available.
- A static route that appears in the routing table only when the primary route goes away is called a floating static route.
  - The administrative distance of the static route is configured to be higher than the administrative distance of the primary route and it “floats” above the primary route, until the primary route is no longer available.
- RIP default administrative distance is 120.
- Static Routes default administrative distance is 1.
  - To create a floating static route (to backup a RIP route) the administrative distance should be greater than 120.
    - In example: 200.

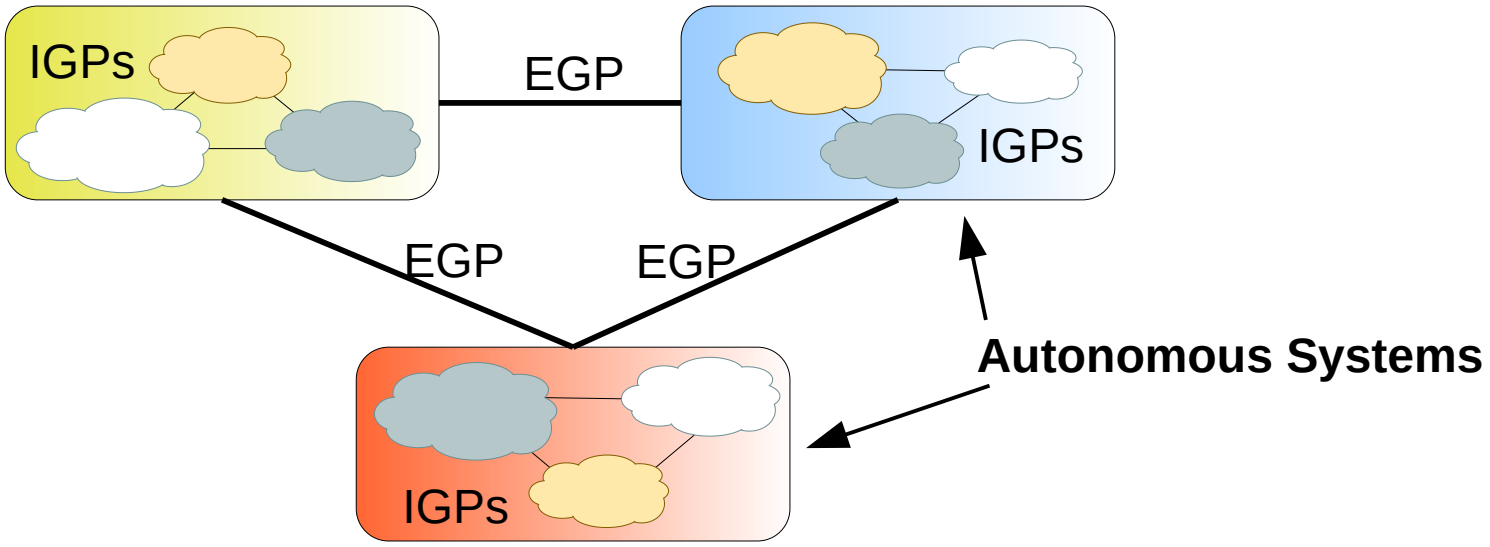



```
ip route 10.0.0.0 255.0.0.0 172.16.1.2 200

router rip
  network 192.168.1.0
  network 172.17.0.0
```

```
ip route 172.17.0.0 255.255.0.0 172.16.1.1 200

router rip
  network 192.168.1.0
  network 10.0.0.0
```

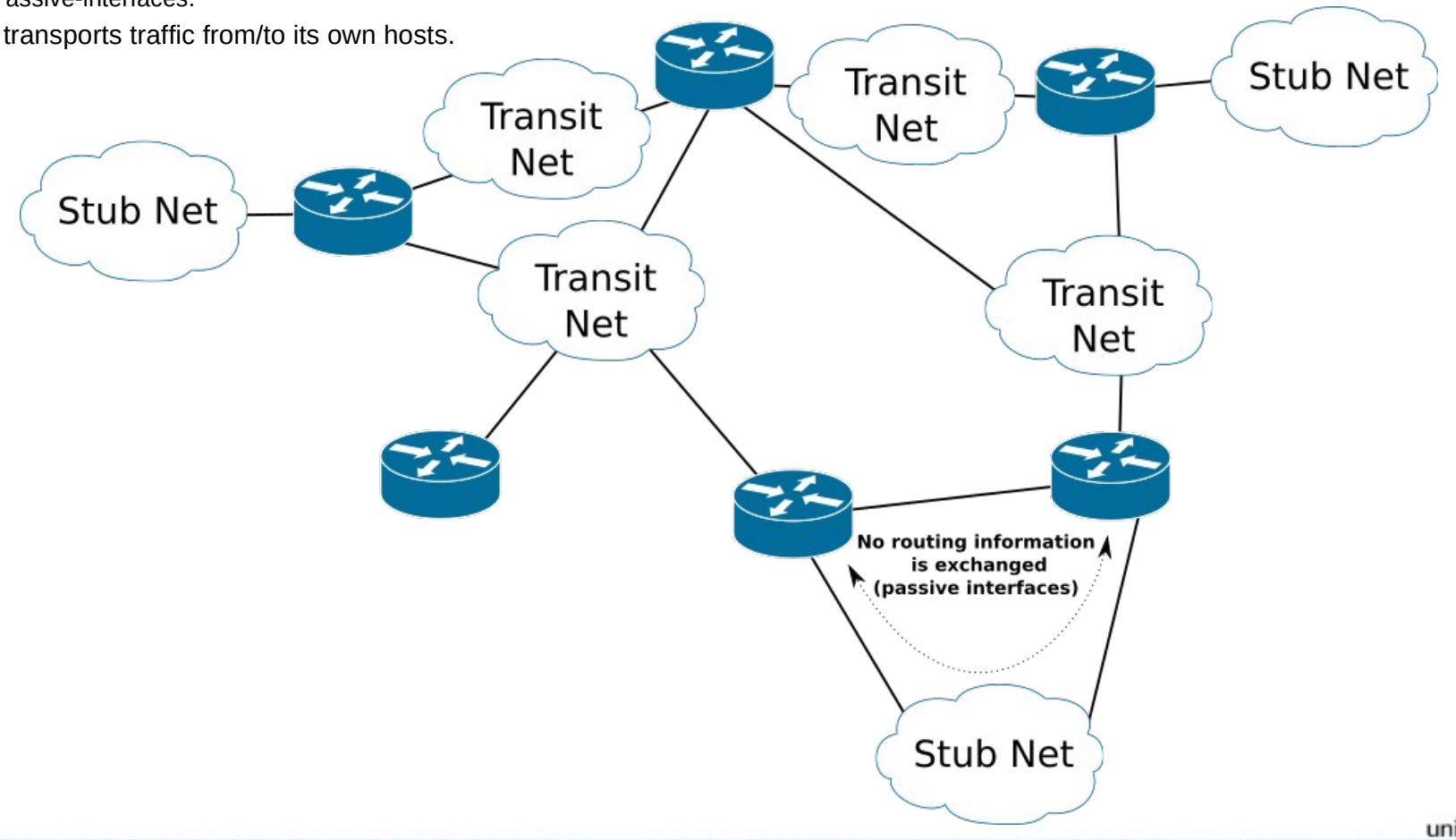
Autonomous Systems

- AS (Autonomous System) – set of routers/networks with a common routing policy and under the same administration.
- Routing inside an AS is performed by IGPs (Interior Gateway Protocols) such as RIPv1, RIPv2, OSPF, IS-IS and EIGRP.
  - Called Internal Routing
- Routing between AS is performed by EGPs (Exterior Gateway Protocols) such as BGP.
- IGPs and EGPs have different objectives:
  - IGPs: optimize routing performance
  - EGPs: optimize routing performance obeying political, economic and security policies.



Type of Networks

- Transit/Transport
  - Used to interconnect networks.
    - Routers exchange routing information using it.
  - Transports traffic from/to other network hosts and from/to its own hosts.
- Stub
  - Single router network.
  - or multiple routers network, if routers do not exchange routing information.
    - Passive-interfaces.
  - Only transports traffic from/to its own hosts.



Distance Vector versus Link State Protocols

- Distance vector
  - Each routers learns networks and best path based on the information sent periodically by its neighbors.
    - Network and cost (distance) to that network.
  - Each router determines the shortest paths to all know networks based on a distributed and asynchronous version of the Bellman-Ford algorithm.
  - Examples: RIPv1, RIPv2, IGRP, EIGRP.
- Link state
  - Routers learn the complete network topology and use a centralized algorithm to determine the shortest paths to all known networks.
  - The information necessary to construct and maintain in each router a data base with the network topology is obtain by a flooding process.
  - Network information is only exchanged on bootstrap and after any topology change.
  - Examples: OSPF, IS-IS.

Open Shortest Path First (OSPF) Protocol

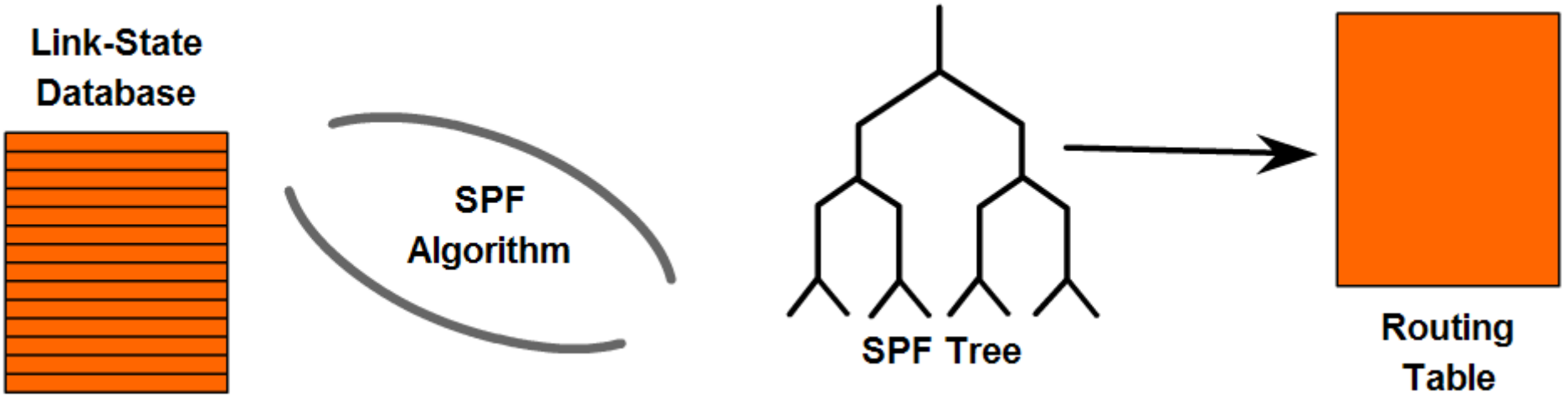
- OSPF is an open-standard protocol based primarily on RFC 2328.
- OSPF is a link-state routing protocol
  - Respond quickly to network changes,
  - Send triggered updates when a network change occurs,
  - Send periodic updates, known as link-state refresh, at long time intervals, such as every 30 minutes.
- Routers running OSPF collect routing information from all other routers in the network (or from within a defined area of the network)
- And then each router independently calculates its best paths to all destinations in the network, using Dijkstra's (SPF) algorithm.

OSPF Necessary Routing Information

- For all the routers in the network to make consistent routing decisions, each link-state router must keep a record of the following information:
  - Its immediate neighbor routers
    - If the router loses contact with a neighbor router, within a few seconds it invalidates all paths through that router and recalculates its paths through the network.
    - For OSPF, adjacency information about neighbors is stored in the OSPF neighbor table, also known as an adjacency database.
  - All the other routers in the network, or in its area of the network, and their attached networks
    - The router recognizes other routers and networks through LSAs, which are flooded through the network.
    - LSAs are stored in a topology table or database (which is also called an LSDB).
  - The best paths to each destination
    - Each router independently calculates the best paths to each destination in the network using Dijkstra's (SPF) algorithm.
    - All paths are kept in the LSDB.
    - The best paths are then offered to the routing table (also called the forwarding database).
    - Packets arriving at the router are forwarded based on the information held in the routing table.

Link-State Protocol Operation

- Link-state routing protocols generate routing updates only when a change occurs in the network topology.
- When a link changes state, the device that detected the change creates a Link-State Advertisement (LSA) concerning that link.
  - LSA propagates to neighbor devices using a special multicast address.
- Each router stores the LSA, forwards the LSA to neighboring devices and updates its Link-State DataBase (LSDB).
- Link-state routers find the best paths to a destination by applying Dijkstra's algorithm, also known as SPF, against the LSDB to build the SPF tree.
- Each router selects the best paths from their SPF tree and places them in their routing table.



Link-State Advertisement (LSA)

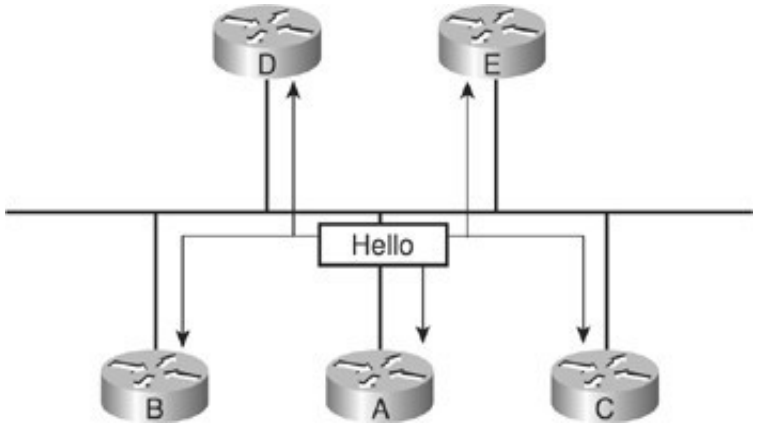
- LSAs report the state of routers and the links between routers.
- Link-state information must be synchronized between routers.
- LSAs have the following characteristics:
  - LSAs are reliable. There is a method for acknowledging their delivery.
  - LSAs are flooded throughout the area (or throughout the domain if there is only one area).
  - LSAs have a sequence number and a set lifetime, so each router recognizes that it has the most current version of the LSA.
  - LSAs are periodically refreshed to confirm topology information before they age out of the LSDB.

OSPF Router ID (RID)

- The Router ID identifies the router and is:
  - The highest IPv4 address of all router interfaces at the moment of the OSPF process activation.
  - A value administratively defined.
- If a physical interface address is being used as the router ID, and that physical interface fails, and the router (or OSPF process) is restarted, the router ID will change.
  - This change in router ID makes it more difficult for network administrators to troubleshoot and manage OSPF.
- Administratively defining the RID or using loopback interfaces for the router ID forces the router ID to stay the same, regardless of the state of the physical interfaces.

OSPF Adjacencies

- A router running a link-state routing protocol must first establish neighbor adjacencies, by exchanging hello packets with the neighboring routers
- The router sends and receives Hello packets to and from its neighboring routers.
  - The destination address is typically a multicast address.
  - It is possible to define unicast OSPF relations.



- The routers exchange hello packets subject to protocol-specific parameters, such as checking whether the neighbor is in the same area, using the same hello interval, and so on.
  - Routers declare the neighbor up when the exchange is complete.
- Two OSPF routers on a point-to-point serial link, usually encapsulated in High-Level Data Link Control (HDLC) or Point-to-Point Protocol (PPP), form a full adjacency with each other.
- However, OSPF routers on broadcast networks, such as LAN links, elect one router as the designated router (DR) and another as the backup designated router (BDR).
  - All other routers on the LAN form full adjacencies with these two routers and pass LSAs only to them.

DR and BDR Election

- The first OSPF router to boot becomes the Designated Router (DR).
- The second router to boot becomes the Backup Designated Router (BDR).
- If multiple routers boot simultaneously,
  - The DR it will be the router with the highest priority. The BDR the second.
    - The OSPF priority is a administratively defined parameter.
  - In case of tie, it will be chosen the router with the highest Router ID (RID).
- When the DR fails, the BDR assumes the role of DR.
  - The BDR does not perform any DR functions when the DR is operating.
  - The choice of the new BDR is done according to some criteria of the initial election.
- After the election, the DR and BDR maintain that role, independently of which routers join the OSPF process.
- The ID of an OSPF Network is the IP address of the network's Designated Router (DR) interface.

OSPF LS Database

- The OSPF database (LSDB) is organized in two tables.
  - Router Link States – Routers related information table.
    - The routers are identified by theirs RID.
  - Net Link States – Networks/Links related information table.
    - Networks are identified by their ID.

```
          OSPF Router with ID (20.20.20.1) (Process ID 1)

         Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
20.20.20.1      20.20.20.1      40          0x8000000A 0x00E7FB 2
30.30.30.2      30.30.30.2      69          0x80000006 0x002906 2
30.30.30.3      30.30.30.3      41          0x80000007 0x00283D 2

         Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.10.10.3      30.30.30.3      41          0x80000001 0x00051C
20.20.20.2      30.30.30.2      70          0x80000001 0x00A164
30.30.30.3      30.30.30.3      154         0x80000001 0x00A91C
```

OSPF LS Database Tables (1)

- Router Link States
  - For each router, it contains the information about the networks directly connected to that router.

```
LS age: 321
Options: (No TOS-capability, DC)
LS Type: Router Links
Link State ID: 20.20.20.1
Advertising Router: 20.20.20.1
LS Seq Number: 8000000A
Checksum: 0xE7FB
Length: 48
Number of Links: 2

  Link connected to: a Transit Network
   (Link ID) Designated Router address: 20.20.20.2
   (Link Data) Router Interface address: 20.20.20.1
    Number of TOS metrics: 0
     TOS 0 Metrics: 1

  Link connected to: a Transit Network
   (Link ID) Designated Router address: 10.10.10.3
   (Link Data) Router Interface address: 10.10.10.1
    Number of TOS metrics: 0
     TOS 0 Metrics: 1
```

Router ID

Number of Links

Network Type

Network ID

Interface IP Address

Interface Cost

OSPF LS Database Tables (2)

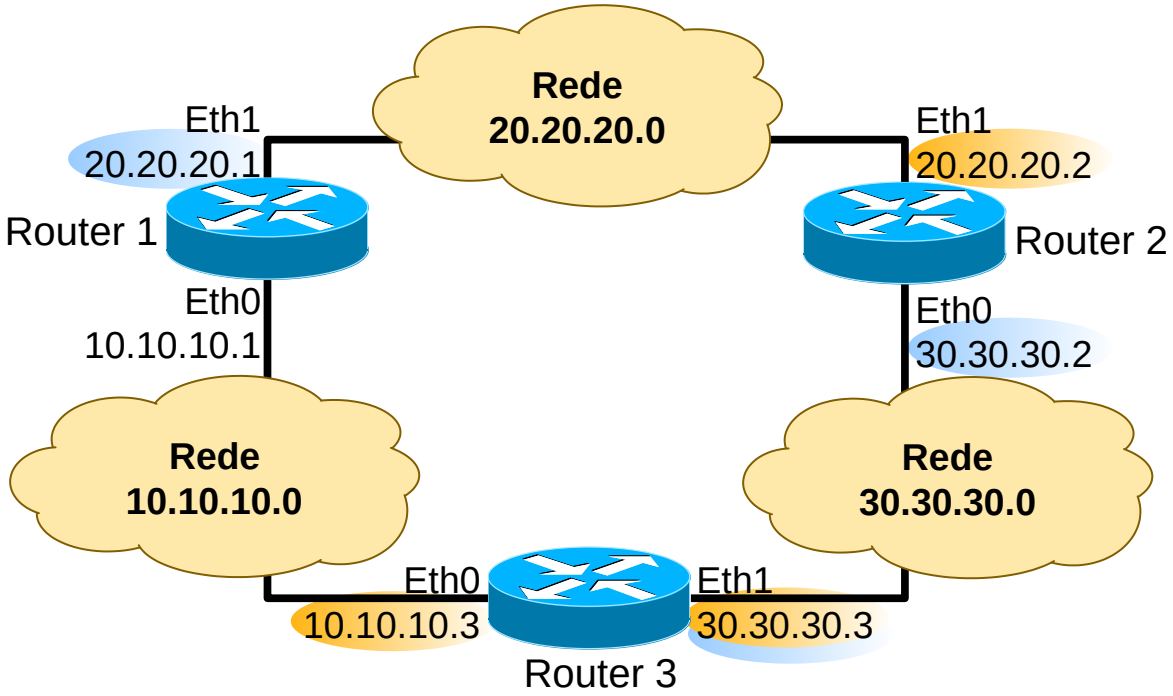
- Network Link States
  - For each network, it contains the information about the routers directly attached to that network.

```
Routing Bit Set on this LSA
LS age: 483
Options: (No TOS-capability, DC)
LS Type: Network Links
Link State ID: 10.10.10.3 (address of Designated Router)
Advertising Router: 30.30.30.3
LS Seq Number: 80000001
Checksum: 0x51C
Length: 32
Network Mask: /24
  Attached Router: 30.30.30.3
  Attached Router: 20.20.20.1
```

Network ID

Attached routers (RID)

OSPF LSDatabase Example




```
 Routing Bit Set on this LSA
  LS age: 208
  Options: (No TOS-capability, DC)
  LS Type: Network Links
  Link State ID: 20.20.20.2 (address of Designated
Router)
  Advertising Router: 30.30.30.2
  LS Seq Number: 80000001
  Checksum: 0xA164
  Length: 32
  Network Mask: /24
Attached Router: 30.30.30.2
Attached Router: 20.20.20.1
```

Network 20.20.20.0's Network Link State

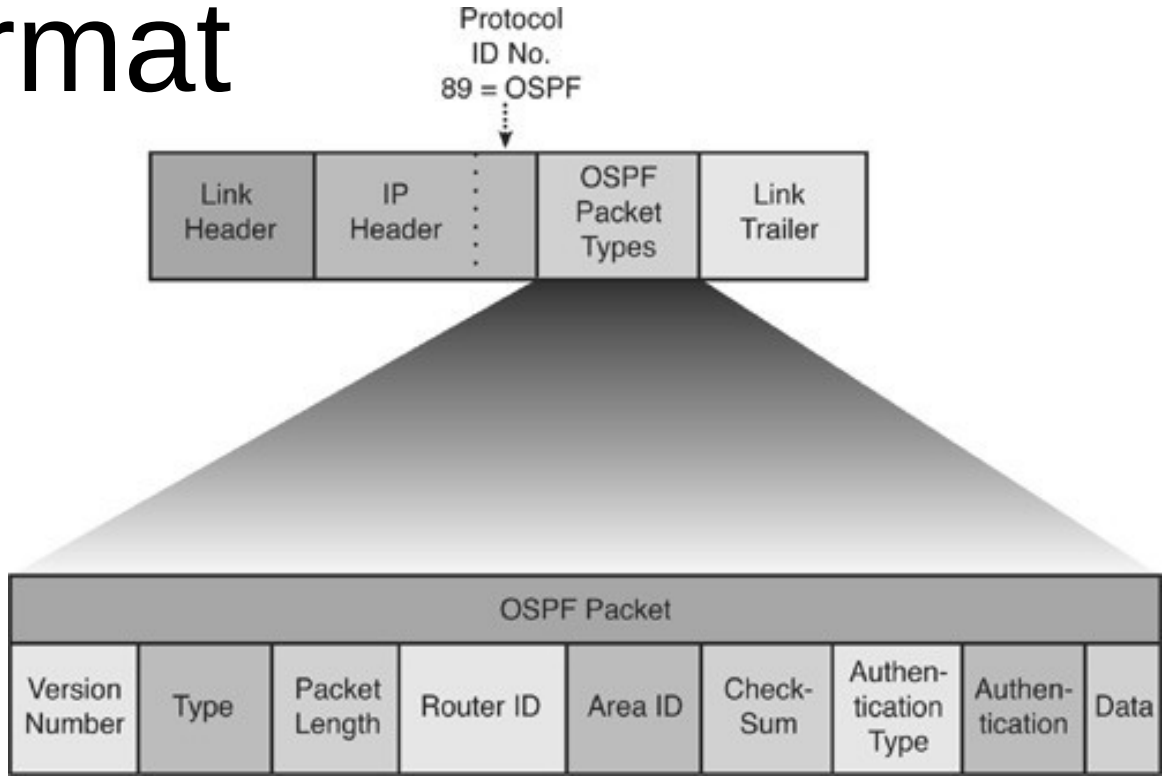
```
LS age: 321
 Options: (No TOS-capability, DC)
 LS Type: Router Links
 Link State ID: 20.20.20.1
 Advertising Router: 20.20.20.1
 LS Seq Number: 8000000A
 Checksum: 0xE7FB
 Length: 48
 Number of Links: 2

   Link connected to: a Transit Network
    (Link ID) Designated Router address: 20.20.20.2
    (Link Data) Router Interface address: 20.20.20.1
     Number of TOS metrics: 0
      TOS 0 Metrics: 1

   Link connected to: a Transit Network
    (Link ID) Designated Router address: 10.10.10.3
    (Link Data) Router Interface address: 10.10.10.1
     Number of TOS metrics: 0
      TOS 0 Metrics: 1
```

Router 1's Router Link State

OSPF Packets

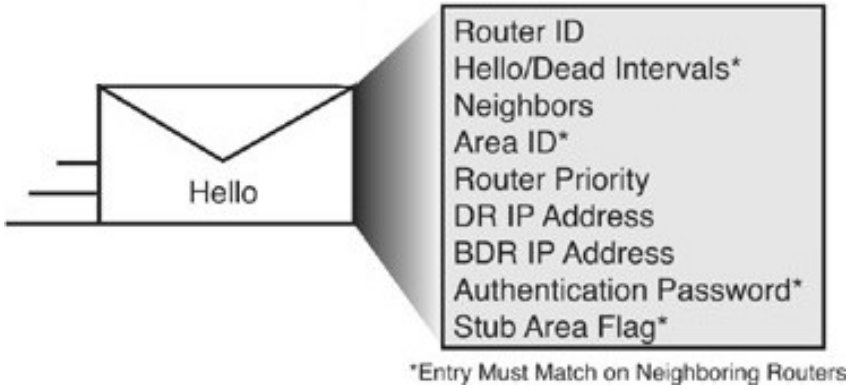
- Hello - Discovers neighbors and builds adjacencies between them.
- Database Description (DBD) - Checks for database synchronization between routers.
- Link-State Request (LSR) - Requests specific link-state records from another router.
- Link-State Update (LSU) - Sends specifically requested link-state records.
- LSAck - Acknowledges the other packet types.

OSPF Packet Format



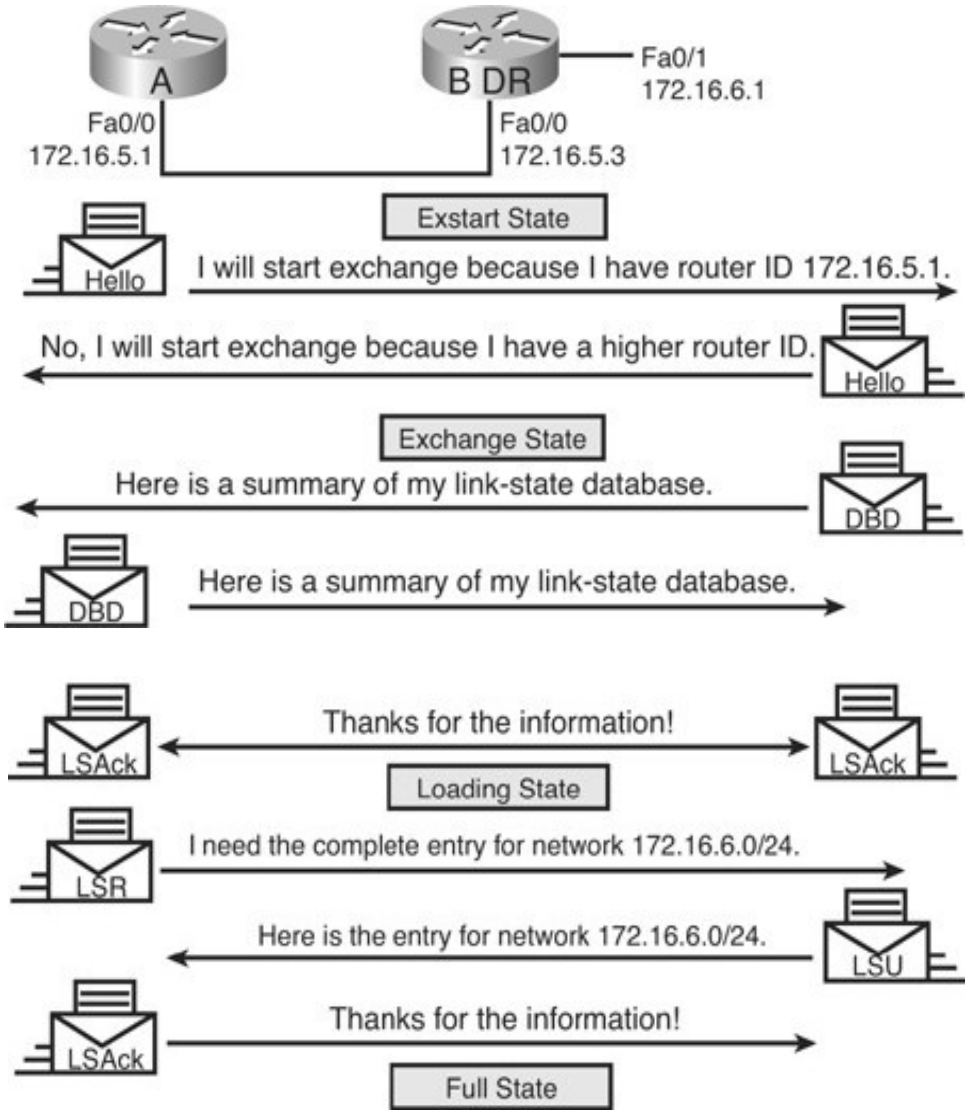
- Version Number
  - Set to 2 for OSPF Version 2, the IPv4 version of OSPF.
  - Set to 3 for OSPF Version 3, the IPv6 version of OSPF.
- Type
  - Differentiates the five OSPF packet types.
- Packet Length
  - The length of the OSPF packet in bytes.
- Router ID
  - Defines which router is the packet's source.
- Area ID
  - Defines the area in which the packet originated.
- Checksum
  - Used for packet header error detection to ensure that the OSPF packet was not corrupted during transmission.
- Authentication Type
  - An option in OSPF that describes either no authentication, clear-text passwords, or encrypted message digest 5 (MD5) for router authentication.
- Authentication
  - Used with authentication type.
- Data, contains different information, depending on the OSPF packet type:
  - For the Hello packet - Contains a list of known neighbors.
  - For the DBD packet - Contains a summary of the LSDB, which includes all known router Ids and their last sequence number, among several other fields.
  - For the LSR packet - Contains the type of LSU needed and the router ID of the router that has the needed LSU.
  - For the LSU packet - Contains the full LSA entries. Multiple LSA entries can fit in one OSPF update packet.
  - For the LSAck packet - This data field is empty.

OSPF Hello Packets



- An hello packet contains the following information:
  - Router ID
    - A 32-bit number that uniquely identifies the router.
  - Hello and dead intervals
    - The hello interval specifies how often, in seconds, a router sends hello packets (10 seconds is the default on multiaccess networks).
    - The dead interval is the amount of time in seconds that a router waits to hear from a neighbor before declaring the neighbor router out of service (the dead interval is four times the hello interval by default).
    - These timers must be the same on neighboring routers; otherwise an adjacency will not be established.
  - Neighbors
    - The Neighbors field lists the adjacent routers with which this router has established bidirectional communication.
    - Bidirectional communication is indicated when the router sees itself listed in the Neighbors field of the hello packet from the neighbor.
  - Area ID
    - To communicate, two routers must share a common segment, and their interfaces must belong to the same OSPF area on that segment.
    - These routers will all have the same link-state information for that area.
  - Router priority
    - An 8-bit number that indicates a router's priority. Priority is used when electing a DR and BDR.
  - DR and BDR IP addresses
    - If known, the IP addresses of the DR and BDR for the specific multiaccess network.
  - Authentication password
    - If router authentication is enabled, two routers must exchange the same password.
    - Authentication is not required, but if it is enabled, all peer routers must have the same password.
  - Stub area flag
    - A stub area is a special area.
    - The stub area technique reduces routing updates by replacing them with a default route.
    - Two neighboring routers must agree on the stub area flag in the hello packets.
- Hello Interval, Dead Interval, Area ID, Authentication Password and Stub Area Flag fields must match on neighboring routers for them to establish an adjacency.

Discovering the Network Routes



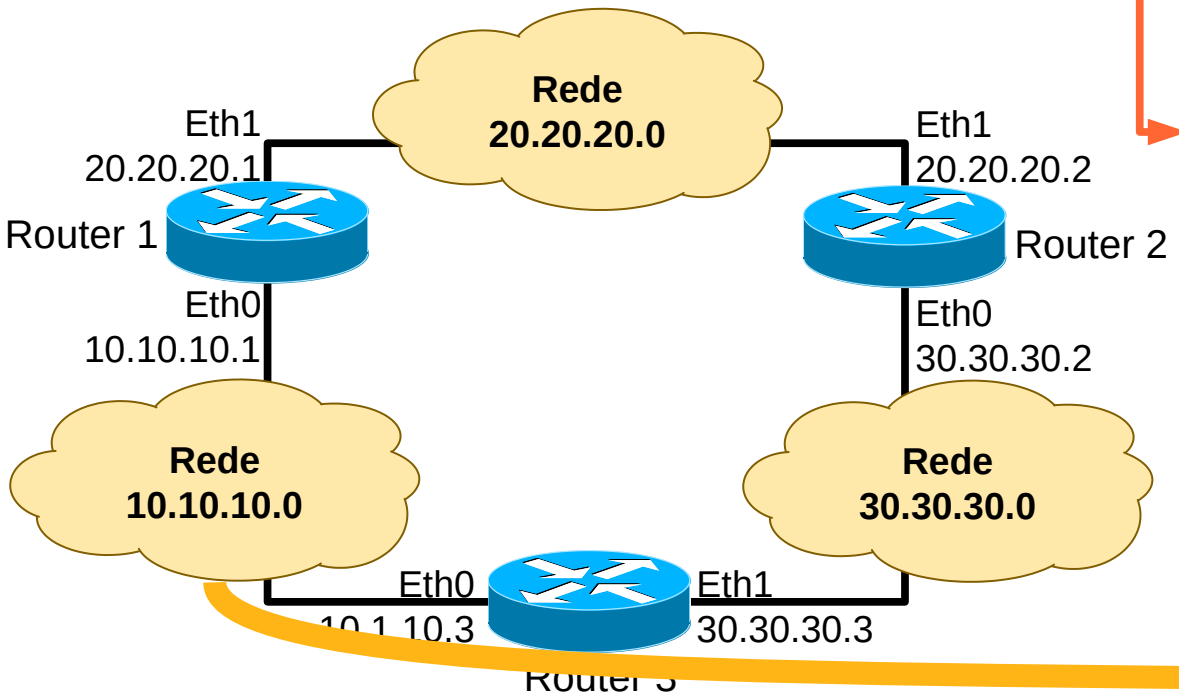
- A master and slave relationship is created between each router and its adjacent DR and BDR.
  - Only the DR exchanges and synchronizes link-state information with the routers to which it has established adjacencies.
- The master and slave routers exchange one or more DBD packets.
  - A DBD includes information about the LSA entry header that appears in the router's LSDB.
  - The entries can be about a link or about a network.
  - Each LSA entry header includes information about the link-state type, the address of the advertising router, the link's cost, and the sequence number.
  - The router uses the sequence number to determine the "newness" of the received link-state information.
- It acknowledges the receipt of the DBD using the LSAck packet.
  - It compares the information it received with the information it has in its own LSDB.
- If the DBD has a more current link-state entry, the router sends an LSR to the other router.
- The other router responds with the complete information about the requested entry in an LSU packet.
- Again, when the router receives an LSU, it sends an LSAck.
- The router adds the new link-state entries to its LSDB.

OSPF Example

OSPF activated on Router 1

OSPF activated on Router 3

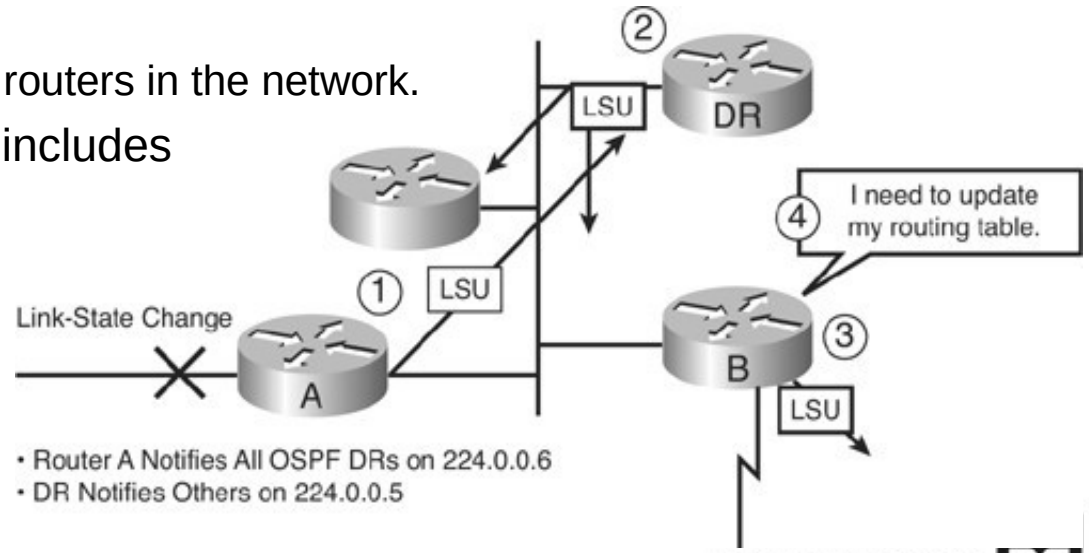
OSPF activated on Router 2



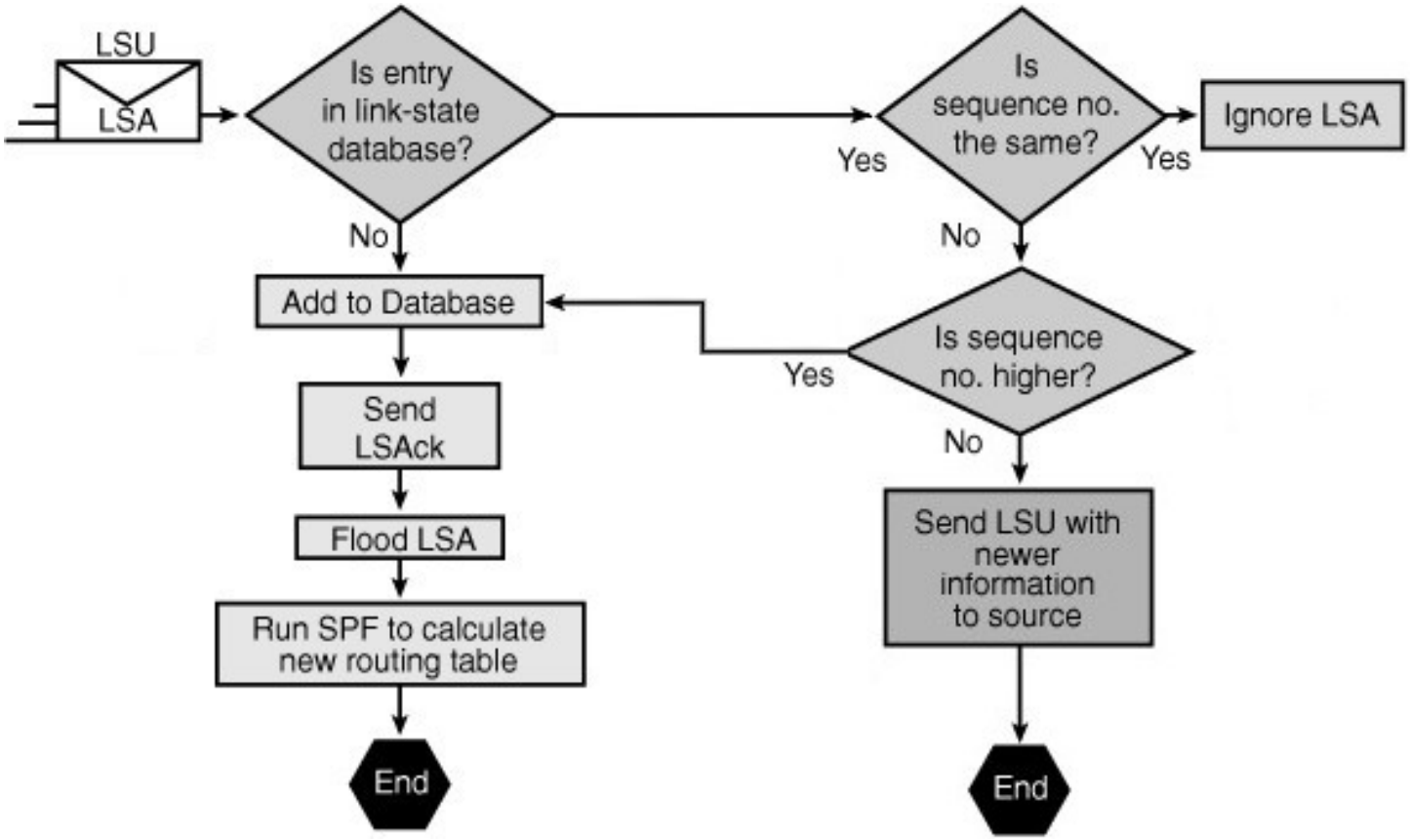

```
     Time  Source        Destination   Protocol Info
  0.000000 10.10.10.1      224.0.0.5   OSPF  Hello Packet
 10.002318 10.10.10.1      224.0.0.5   OSPF  Hello Packet
 20.003116 10.10.10.1      224.0.0.5   OSPF  Hello Packet
----------
 80.000000 10.10.10.3      224.0.0.5   OSPF  Hello Packet
 83.683033 10.10.10.3      224.0.0.5   OSPF  LS Update
 83.715683 10.10.10.3      224.0.0.5   OSPF  Hello Packet
 83.717864 10.10.10.1      10.10.10.3  OSPF  Hello Packet
 83.726166 10.10.10.3      10.10.10.1  OSPF  DB Descr.
 83.726258 10.10.10.3      10.10.10.1  OSPF  Hello Packet
 83.728433 10.10.10.1      10.10.10.3  OSPF  DB Descr.
 83.732590 10.10.10.3      10.10.10.1  OSPF  DB Descr.
 83.734733 10.10.10.1      10.10.10.3  OSPF  DB Descr.
 83.738942 10.10.10.3      10.10.10.1  OSPF  LS Request
 83.741083 10.10.10.1      10.10.10.3  OSPF  LS Update
 84.240362 10.10.10.3      224.0.0.5   OSPF  LS Update
 86.245792 10.10.10.3      224.0.0.5   OSPF  LS Acknowledge
 86.380876 10.10.10.1      224.0.0.5   OSPF  Hello Packet
 86.741036 10.10.10.1      224.0.0.5   OSPF  LS Acknowledge
 93.721376 10.10.10.3      224.0.0.5   OSPF  Hello Packet
 96.380005 10.10.10.1      224.0.0.5   OSPF  Hello Packet
----------
213.780338 10.10.10.3      224.0.0.5   OSPF  Hello Packet
216.542473 10.10.10.1      224.0.0.5   OSPF  Hello Packet
216.568852 10.10.10.1      224.0.0.5   OSPF  LS Update
217.048427 10.10.10.1      224.0.0.5   OSPF  LS Update
217.084909 10.10.10.1      224.0.0.5   OSPF  LS Update
219.067748 10.10.10.3      224.0.0.5   OSPF  LS Acknowledge
219.650308 10.10.10.1      224.0.0.5   OSPF  LS Update
222.150349 10.10.10.3      224.0.0.5   OSPF  LS Acknowledge
223.779492 10.10.10.3      224.0.0.5   OSPF  Hello Packet
224.284149 10.10.10.3      224.0.0.5   OSPF  LS Update
224.789598 10.10.10.1      224.0.0.5   OSPF  LS Update
224.789775 10.10.10.3      224.0.0.5   OSPF  LS Update
226.545718 10.10.10.1      224.0.0.5   OSPF  Hello Packet
226.785254 10.10.10.1      224.0.0.5   OSPF  LS Acknowledge
227.294756 10.10.10.3      224.0.0.5   OSPF  LS Acknowledge
233.779863 10.10.10.3      224.0.0.5   OSPF  Hello Packet
236.544658 10.10.10.1      224.0.0.5   OSPF  Hello Packet
```

Maintaining Routing Information

- Flooding process:
  - A router notices a change in a link state and multicasts an LSU packet, which includes the updated LSA entry with the sequence number incremented, to 224.0.0.6.
    - This address goes to all OSPF DRs and BDRs.
    - On point-to-point links, the LSU is multicast to 224.0.0.5.)
    - An LSU packet might contain several distinct LSAs.
  - The DR receives the LSU, processes it, acknowledges the receipt of the change and floods the LSU to other routers on the network using the OSPF multicast address 224.0.0.5.
    - After receiving the LSU, each router responds to the DR with an LSAck.
    - To make the flooding procedure reliable, each LSA must be acknowledged separately.
  - If a router is connected to other networks, it floods the LSU to those other networks by forwarding the LSU to the DR of the other network (or to the adjacent router if in a point-to-point network).
    - That DR, in turn, multicasts the LSU to the other routers in the network.
  - The router updates its LSDB using the LSU that includes the changed LSA.
  - It then recomputes the SPF algorithm against the updated database after a short delay and updates the routing table as necessary.



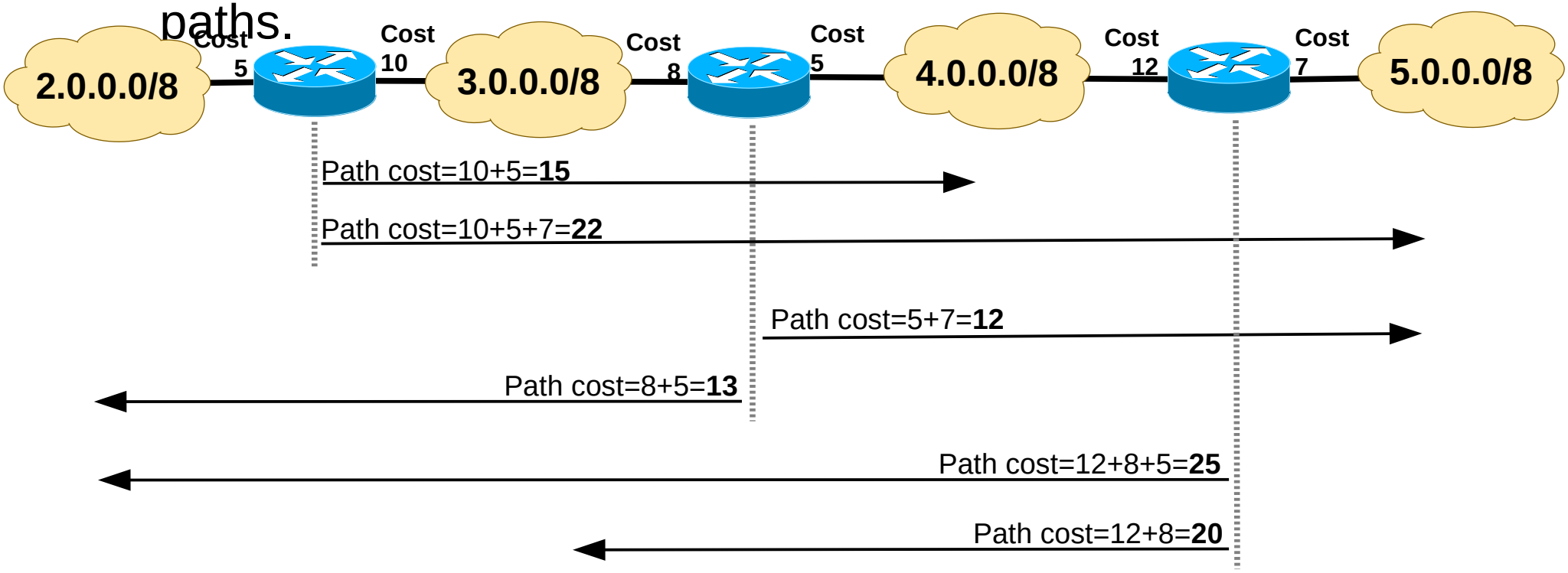
LSA Operation



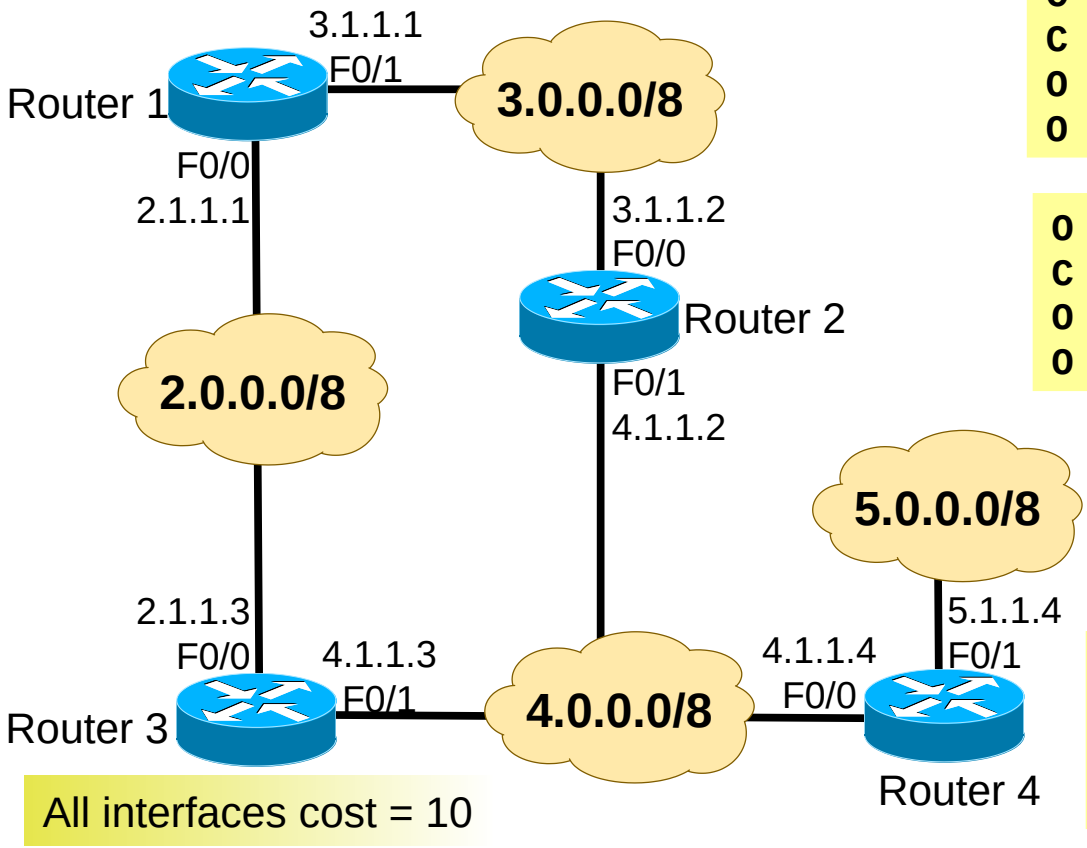
- When each router receives the LSU:
  - If the LSA entry does not already exist, the router adds the entry to its LSDB, sends back a link-state acknowledgment (LSAck), floods the information to other routers, runs SPF, and updates its routing table.
  - If the entry already exists and the received LSA has the same sequence number, the router ignores the LSA entry.
  - If the entry already exists but the LSA includes newer information (it has a higher sequence number), the router adds the entry to its LSDB, sends back an LSAck, floods the information to other routers, runs SPF, and updates its routing table.
  - If the entry already exists but the LSA includes older information, it sends an LSU to the sender with its newer information.

OSPF Path Costs

- Each router link/interface has an associated OSPF cost.
- The total cost between a router and a network is given by the sum of all OSPF costs of the (routers) output interfaces along the path.
  - Routers to access directly connect networks never use OSPF paths.



OSPF Example




```
C  2.0.0.0/8 is directly connected, F0/0
C  3.0.0.0/8 is directly connected, F0/1
O  4.0.0.0/8 [110/20] via 2.1.1.3, 00:01:18, F0/0
O  5.0.0.0/8 [110/30] via 2.1.1.3, 00:01:00, F0/0
```

```
O  2.0.0.0/8 [110/20] via 3.1.1.1, 00:01:13, F0/0
C  3.0.0.0/8 is directly connected, F0/0
O  4.0.0.0/8 [110/30] via 3.1.1.1, 00:01:13, F0/0
O  5.0.0.0/8 [110/40] via 3.1.1.1, 00:01:10, F0/0
```

Router 1 and Router 2 after disconnecting the F0/1 at Router2

```
C  2.0.0.0/8 is directly connected, F0/0
C  3.0.0.0/8 is directly connected, F0/1
O  4.0.0.0/8 [110/15] via 3.1.1.2, 00:01:13, F0/1
O  5.0.0.0/8 [110/25] via 3.1.1.2, 00:01:10, F0/1
```

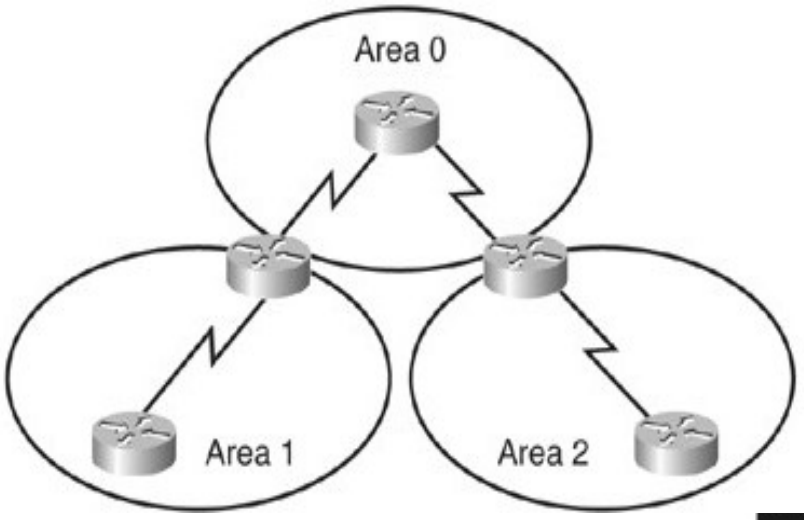
Router1, now with the cost of Router2 F0/1 interface equal to 5

```
C  2.0.0.0/8 is directly connected, F0/0
C  3.0.0.0/8 is directly connected, F0/1
O  4.0.0.0/8 [110/20] via 3.1.1.2, 00:01:13, F0/1
             [110/20] via 2.1.1.3, 00:01:31, F0/0
O  5.0.0.0/8 [110/30] via 3.1.1.2, 00:01:10, F0/1
             [110/30] via 2.1.1.3, 00:01:10, F0/0
```

Router 1 initial table

OSPF Hierarchical Routing (1)

- In small networks, the web of router links is not complex, and paths to individual destinations are easily deduced.
- In large networks, the resulting web is highly complex, and the number of potential paths to each destination is large.
  - Dijkstra calculations comparing all of these possible routes can be very complex and can take significant time.
    - Large LSDB. Because the LSDB covers the topology of the entire network, each router must maintain an entry for every network in the area, even if not every route is selected for the routing table.
    - Frequent SPF algorithm calculations. In a large network, changes are inevitable, so the routers spend many CPU cycles recalculating the SPF algorithm and updating the routing table.
    - Large routing table. OSPF does not perform route summarization by default. If the routes are not summarized, the routing tables can become very large, depending on the size of the network.
- Link-state routing protocols usually reduce the size of the Dijkstra calculations by partitioning the network into areas.



OSPF Hierarchical Routing (2)

- Using multiple OSPF areas has several important advantages:
  - Reduced frequency of SPF calculations.
    - Detailed route information only exists within each area
    - It is not necessary to flood all link-state changes to all other areas.
    - Only routers that are affected by the change need to recalculate the SPF algorithm and the impact of the change is localized within the area.
  - Reduced updates overhead.
    - Rather than send an update about each network within an area, a router can advertise a single summarized route or a small number of routes between areas, thereby reducing the overhead associated with updates when they cross areas.
  - Smaller routing tables.
    - Detailed route entries for specific networks within an area can remain in the area.
    - Routers can be configured to summarize the routes into one or more summary addresses.
    - Advertising these summaries reduces the number of messages propagated between areas but keeps all networks reachable.

Integrated System-Integrated System (IS-IS) Protocol

- IS-IS was defined in 1992 in the ISO/IEC recommendation 10589.
- IS-IS is a link-state routing protocol.
  - Provides fast convergence and excellent scalability.
  - Very efficient in its use of network bandwidth.
- Uses Dijkstra's Shortest Path First algorithm (SPF).
- Types of packets
  - IS-IS Hello packet (IIH), Link State Packet (LSP), Partial Sequence Number Packet (PSNP) and Complete Sequence Number Packet (CSNP).
- Link States are called LSPs
  - Contain all information about one router adjacencies, connected IP prefixes, OSI end systems, area addresses, etc.
  - One LSP per router (plus fragments).
  - One LSP per LAN network.
- IS-IS has 2 layers of hierarchy
  - The backbone is called level-2.
  - Areas are called level-1.
  - A router can take part in L1 and L2 inter-area routing (or inter-level routing).

Enhanced Interior Gateway Routing Protocol (EIGRP) Protocol

- EIGRP is a Cisco-proprietary protocol that combines the advantages of link-state and distance vector routing protocols.
- EIGRP has its roots as a distance vector routing protocol and is predictable in its behavior.
- What makes EIGRP an advanced distance vector protocol is the addition of several link-state features, such as dynamic neighbor discovery.
  - EIGRP Maintains a Neighbor Table, a Topology Table, and a Routing Table.
- EIGRP has Variable-length subnet masking (VLSM) support.
- Has a sophisticated metric that considers five criteria:
  - Two by default:
    - Bandwidth - The smallest (slowest) bandwidth between the source and destination.
    - Delay - The cumulative interface delay along the path.
  - Available, are not commonly used, because they typically result in frequent recalculation of the topology table:
    - Reliability - The worst reliability between the source and destination, based on keepalives.
    - Loading - The worst load on a link between the source and destination based on the packet rate and the interface's configured bandwidth.
    - Maximum transmission unit (MTU) - The smallest MTU in the path.
- A significant advantage of EIGRP (and IGRP) over other protocols is its support for unequal metric load balancing that allows administrators to better distribute traffic flow in their networks.

RIPng for IPv6 Routing

- Similar to IPv4 RIPv2:
  - Distance-vector concept, radius of 15 hops, infinity metric is 16, split-horizon, triggered update.
- Differences between RIPv2 and RIPng
  - Uses IPv6 for transport.
    - Uses link-local addresses (not the global ones).
  - IPv6 prefix, next-hop IPv6 link-local address.
  - Uses multicast group address FF02::9 (all-RIP-routers) as the destination address for RIP updates.
  - Routers always add the cost of the interface to the metric received.
    - Metric is sum of “output interfaces” costs to destination and not number of hops.
    - If all costs are 1, metric is number of “output interfaces” to destination.
  - Allows for node/interface costs other than 1.
    - Cisco calls it “cost offset” per interface (out or in direction).
    - Cost to network is given by the sum of all output interfaces costs along the path.
    - With the infinity metric value at 16, this require careful configurations.
  - Routers always announce directed connected networks.
  - in IOS Cisco
    - Activation per interface, named process, more than one active process.

IPv6 Routing Tables with RIPng

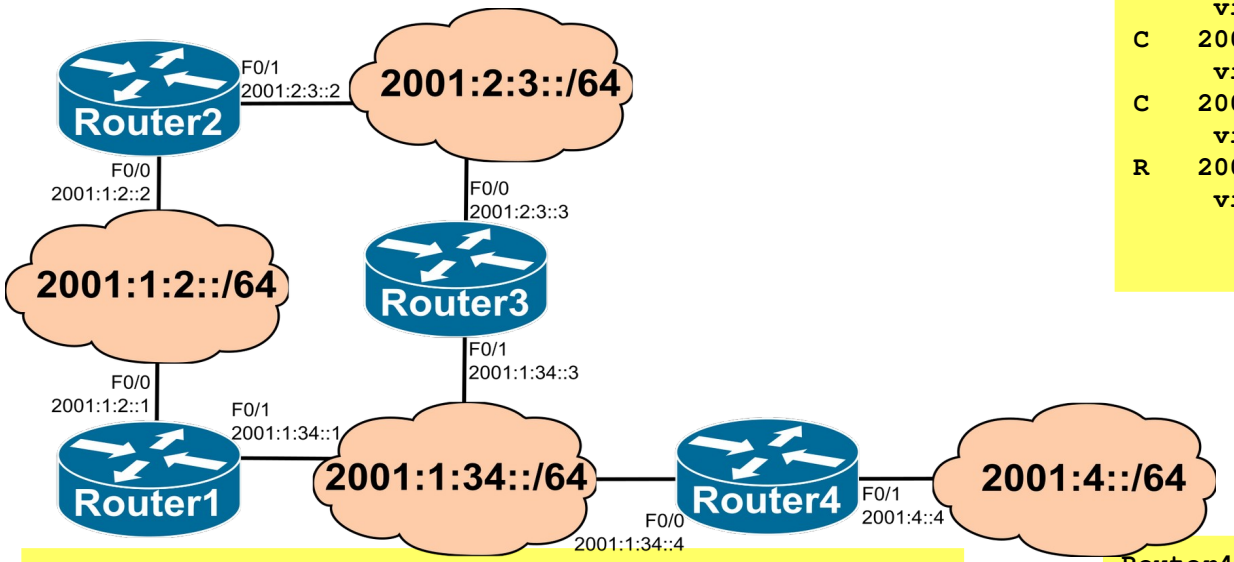
Router2

```
C   2001:1:2::/64 [0/0]
     via FastEthernet0/0, directly connected
R   2001:1:34::/64 [120/2]
     via FE80::C801:54FF:FE41:8, FastEthernet0/0
     via FE80::C803:56FF:FE0A:8, FastEthernet0/1
C   2001:2:3::/64 [0/0]
     via FastEthernet0/1, directly connected
R   2001:4::/64 [120/3]
     via FE80::C801:54FF:FE41:8, FastEthernet0/0
     via FE80::C803:56FF:FE0A:8, FastEthernet0/1
```

Assuming all interfaces with cost 1.

Router3

```
R   2001:1:2::/64 [120/2]
     via FE80::C802:54FF:FEF5:6, FastEthernet0/0
     via FE80::C801:54FF:FE41:6, FastEthernet0/1
C   2001:1:34::/64 [0/0]
     via FastEthernet0/1, directly connected
C   2001:2:3::/64 [0/0]
     via FastEthernet0/0, directly connected
R   2001:4::/64 [120/2]
     via FE80::C804:56FF:FEAD:8, FastEthernet0/1
```



Router1

```
C   2001:1:2::/64 [0/0]
     via FastEthernet0/0, directly connected
C   2001:1:34::/64 [0/0]
     via FastEthernet0/1, directly connected
R   2001:2:3::/64 [120/2]
     via FE80::C802:54FF:FEF5:8, FastEthernet0/0
     via FE80::C803:56FF:FE0A:6, FastEthernet0/1
R   2001:4::/64 [120/2]
     via FE80::C804:56FF:FEAD:8, FastEthernet0/1
```

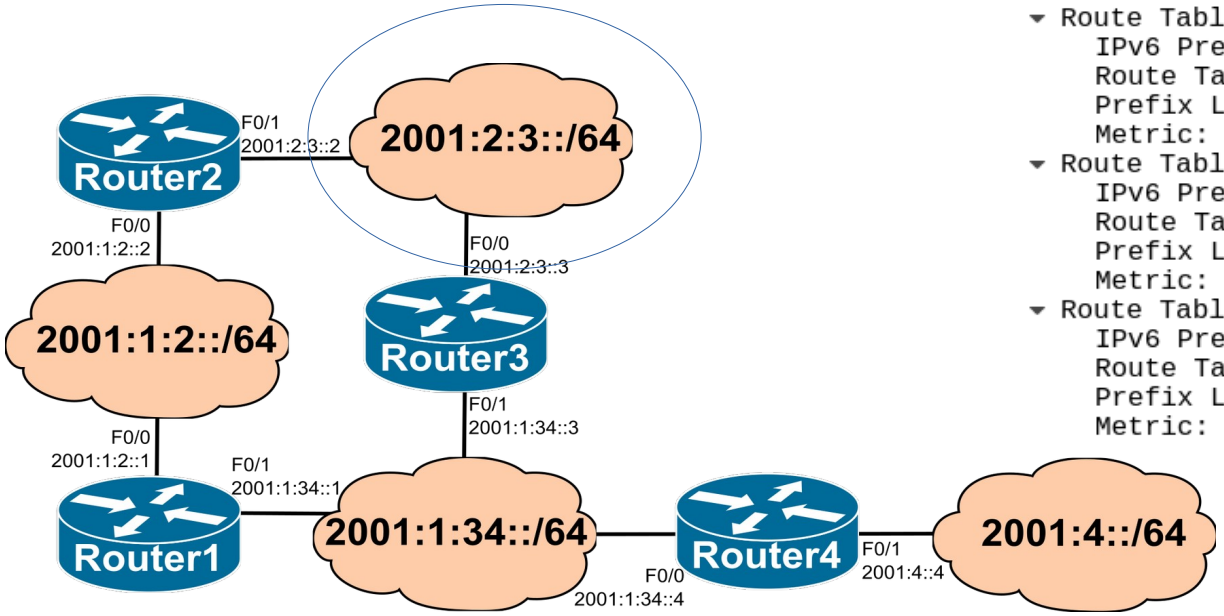
Router4

```
R   2001:1:2::/64 [120/2]
     via FE80::C801:54FF:FE41:6, FastEthernet0/0
C   2001:1:34::/64 [0/0]
     via FastEthernet0/0, directly connected
R   2001:2:3::/64 [120/2]
     via FE80::C803:56FF:FE0A:6, FastEthernet0/0
C   2001:4::/64 [0/0]
     via FastEthernet0/1, directly connected
```

RIPng Messages (Example)

Sent by Router2 with Split-Horizon

```
▸ Internet Protocol Version 6, Src: fe80::c802:54ff:fef5:6, Dst: ff02::9
▸ User Datagram Protocol, Src Port: 521, Dst Port: 521
▾ RIPng
    Command: Response (2)
    Version: 1
    Reserved: 0000
  ▾ Route Table Entry: IPv6 Prefix: 2001:1:2::/64 Metric: 1
      IPv6 Prefix: 2001:1:2::
      Route Tag: 0x0000
      Prefix Length: 64
      Metric: 1
  ▾ Route Table Entry: IPv6 Prefix: 2001:2:3::/64 Metric: 1
      IPv6 Prefix: 2001:2:3::
      Route Tag: 0x0000
      Prefix Length: 64
      Metric: 1
```



Sent by Router3 with Split-Horizon

```
▸ Internet Protocol Version 6, Src: fe80::c803:56ff:fe0a:8, Dst: ff02::9
▸ User Datagram Protocol, Src Port: 521, Dst Port: 521
▾ RIPng
    Command: Response (2)
    Version: 1
    Reserved: 0000
  ▾ Route Table Entry: IPv6 Prefix: 2001:2:3::/64 Metric: 1
      IPv6 Prefix: 2001:2:3::
      Route Tag: 0x0000
      Prefix Length: 64
      Metric: 1
  ▾ Route Table Entry: IPv6 Prefix: 2001:1:34::/64 Metric: 1
      IPv6 Prefix: 2001:1:34::
      Route Tag: 0x0000
      Prefix Length: 64
      Metric: 1
  ▾ Route Table Entry: IPv6 Prefix: 2001:4::/64 Metric: 2
      IPv6 Prefix: 2001:4::
      Route Tag: 0x0000
      Prefix Length: 64
      Metric: 2
```

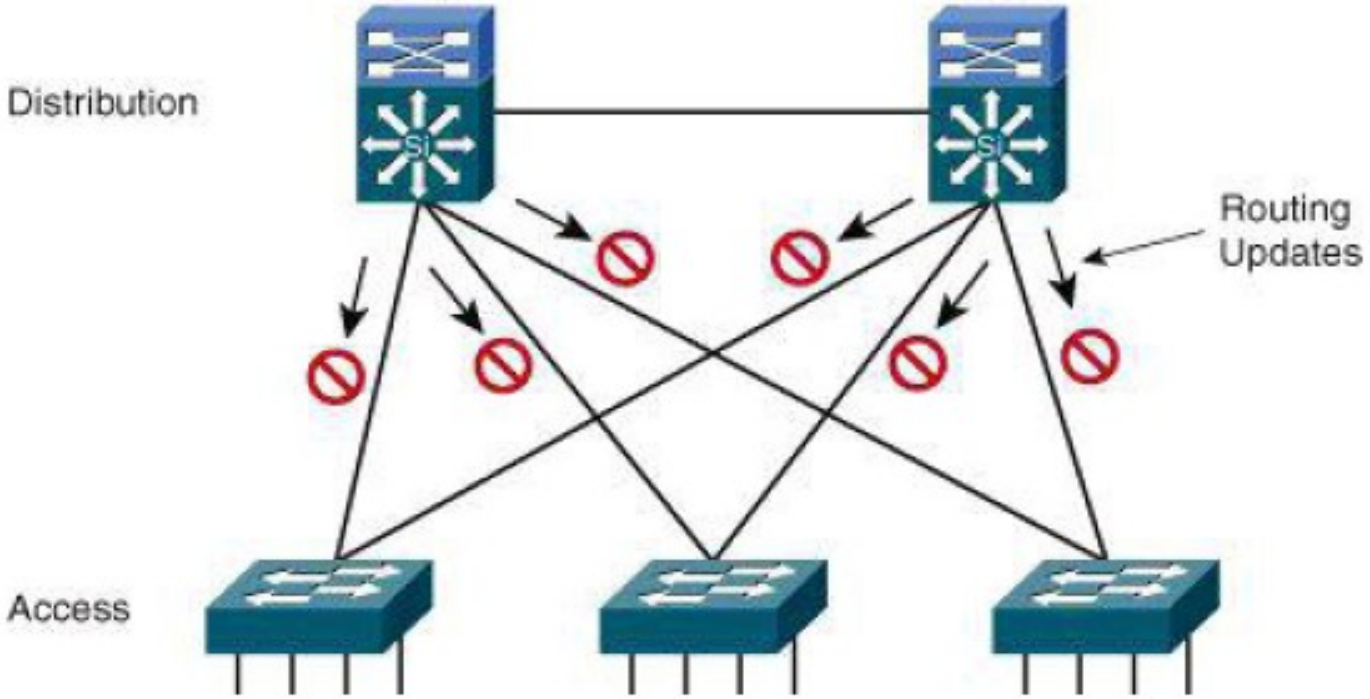
Routing - OSPFv3

- Based on OSPFv2, with enhancements:
  - Uses IPv6 for transport
  - Distributes IPv6 prefixes
  - Uses multicast group addresses FF02::5 (OSPF IGP) and FF02::6 (OSPF IGP Designated Routers)
  - Runs over a link rather than a subnet
  - Multiple instances per link
  - Topology not IPv6-specific
    - Router ID, Area ID, Link ID remain a 4 bytes number
    - Neighbors are always identified by Router ID (4 bytes)
    - With an additional table with mapping between IPv6 prefixes and Link IDs
  - Uses link-local addresses as IPv6 source addresses

OSPFv3 - LSA Types

- Link LSA (Type 8)
  - Informs neighbors of link local address
  - Informs neighbors of IPv6 prefixes on link
- Intra-Area Prefix LSA (Type 9)
  - Associates IPv6 prefixes with a network or router
- Flooding scope for LSAs has been generalized
  - Three flooding scopes for LSAs
    - Link-local
    - Area
    - AS
- LSA Type encoding expanded to 16 bits
  - Includes flooding scope

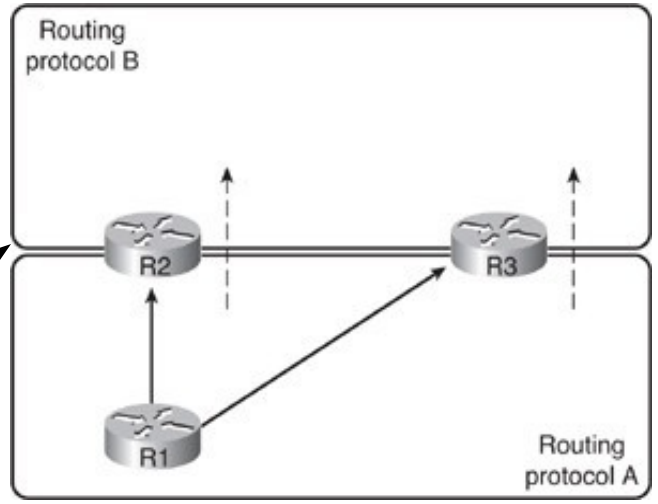
Passive Interfaces on Access Layer

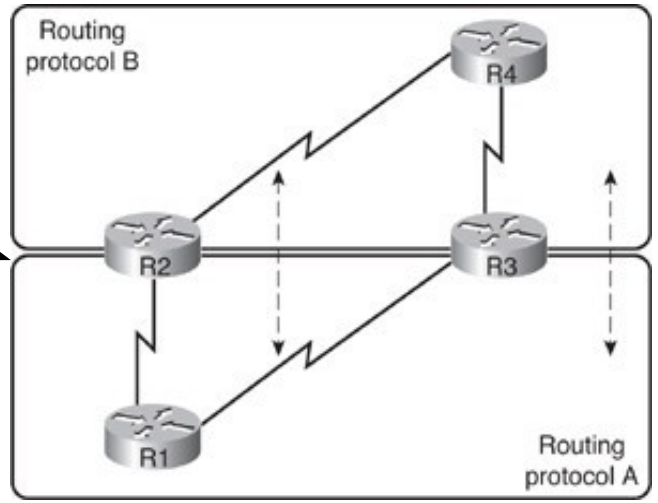


- As a recommended practice, limit unnecessary L3 routing peer adjacencies by configuring the ports toward Layer 2 access switches as passive.
  - Suppress the advertising of routing updates.
  - If a distribution switch does not receive L3 routing updates from a potential peer on a specific interface, it does not form a neighbor adjacency with the potential peer across that interface.

Route Redistribution

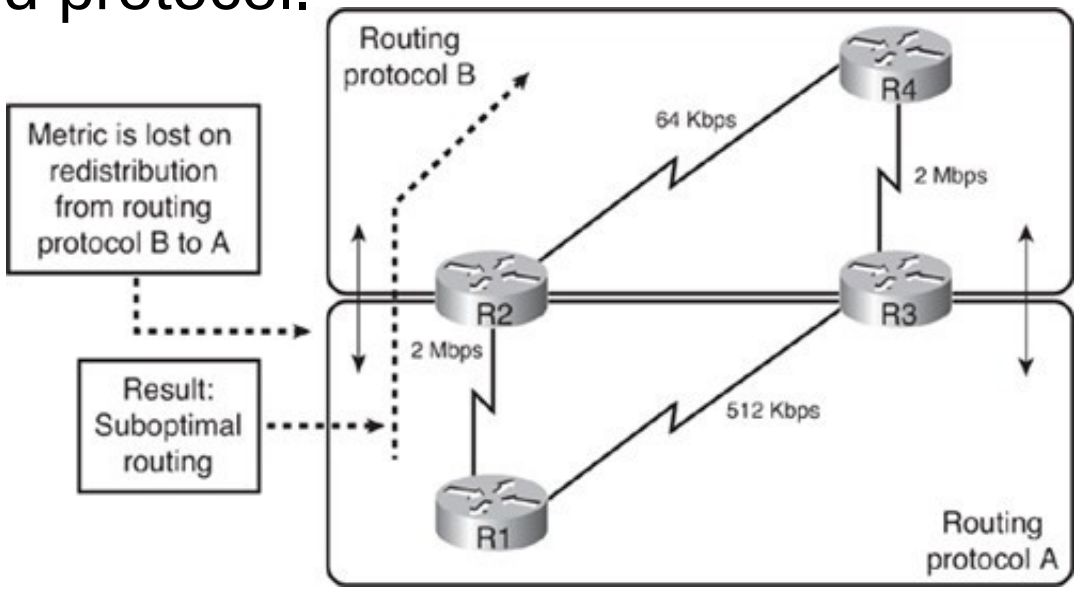
- Domains with difference routing protocols can exchange routes.
  - This is called route redistribution.
    - One-way redistribution - Redistributes only the networks learned from one routing protocol into the other routing protocol.
      - Uses a default or static route so that devices in that other part of the network can reach the first part of the network
    - Two-way redistribution - Redistributes routes between the two routing processes in both directions
  - Static routes can also be redistributed.





Redistribution Issues

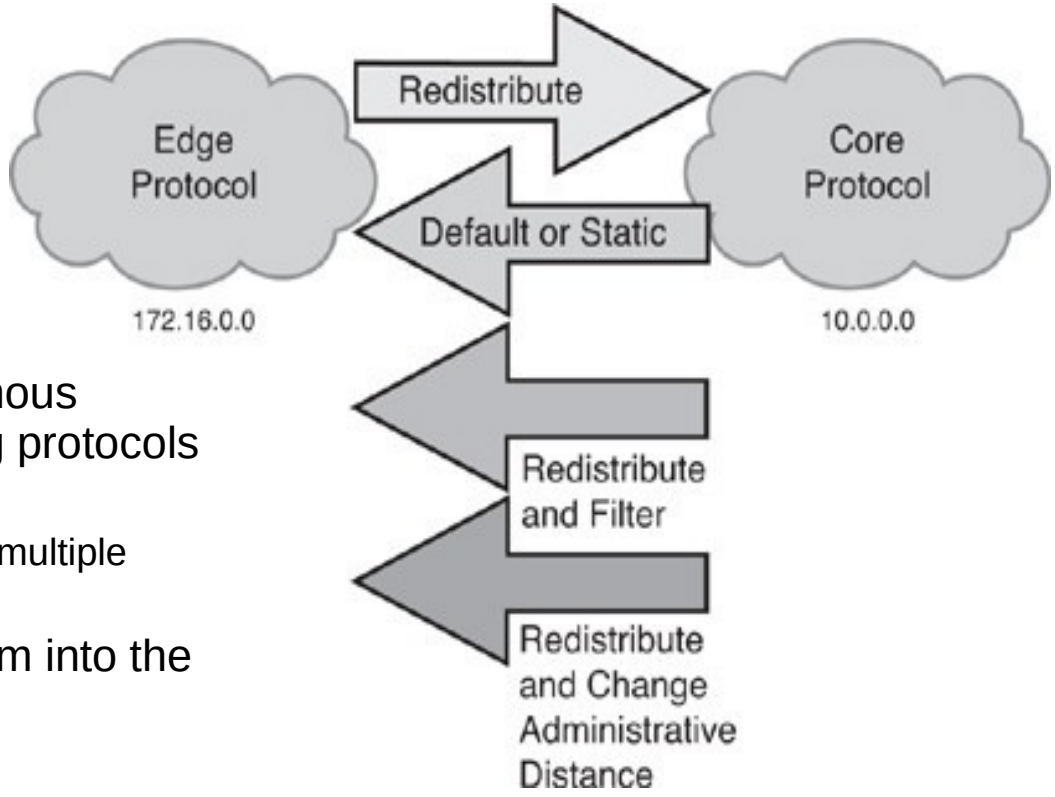
- Lost metric from redistributed protocol.
  - It is not possible to achieve an optimal overall routing.



- Preventing Routing Loops in a Redistribution Environment.
  - Safest way to perform redistribution is to redistribute routes in only one direction, on only one boundary router within the network.
    - However, that this results in a single point of failure in the network.
  - If redistribution must be done in both directions or on multiple boundary routers, the redistribution should be tuned to avoid problems such as suboptimal routing and routing loops.

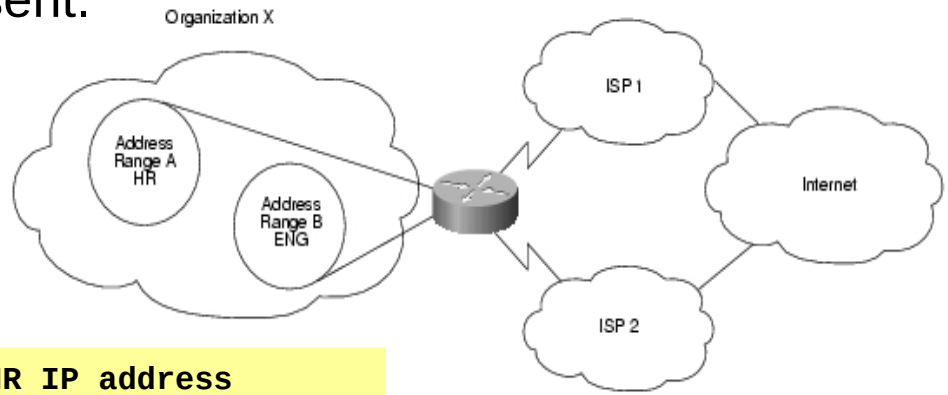
Redistribution Techniques

- Redistribute a default route from the core autonomous system into the edge autonomous system, and redistribute routes from the edge routing protocols into the core routing protocol.
  - This technique helps prevent route feedback, suboptimal routing, and routing loops.
- Redistribute multiple static routes about the core autonomous system networks into the edge autonomous system, and redistribute routes from the edge routing protocols into the core routing protocol.
  - This method works if there is only one redistribution point; multiple redistribution points might cause route feedback.
- Redistribute routes from the core autonomous system into the edge autonomous system with filtering to block out inappropriate routes.
  - For example, when there are multiple boundary routers, routes redistributed from the edge autonomous system at one boundary router should not be redistributed back into the edge autonomous system from the core at another redistribution point.
- Redistribute all routes from the core autonomous system into the edge autonomous system, and from the edge autonomous system into the core autonomous system, and then modify the administrative distance associated with redistributed routes so that they are not the selected routes when multiple routes exist for the same destination.



Policy-Based Routing (PBR)

- PBR allows the operator to define routing policy other than basic destination-based routing using the routing table.
- PBR rules can be used to match source and destination addresses, protocol types, and end-user applications.
- When a match occurs, a set command can be used to define the interface or next-hop address to which the packet should be sent.




```
access-list 1 permit 209.165.200.225        !From HR IP address
access-list 2 permit 209.165.200.226        !From ENG IP address
!
interface ethernet 1
 ip policy route-map ChooseISP
!
route-map ChooseISP permit 10
 match ip address 1
 set ip next-hop 209.165.200.227            !To ISP2 next-hop
!
route-map ChooseISP permit 20
 match ip address 2
 set ip next-hop 209.165.200.228            !To ISP1 next-hop
```

Defines order of the rules

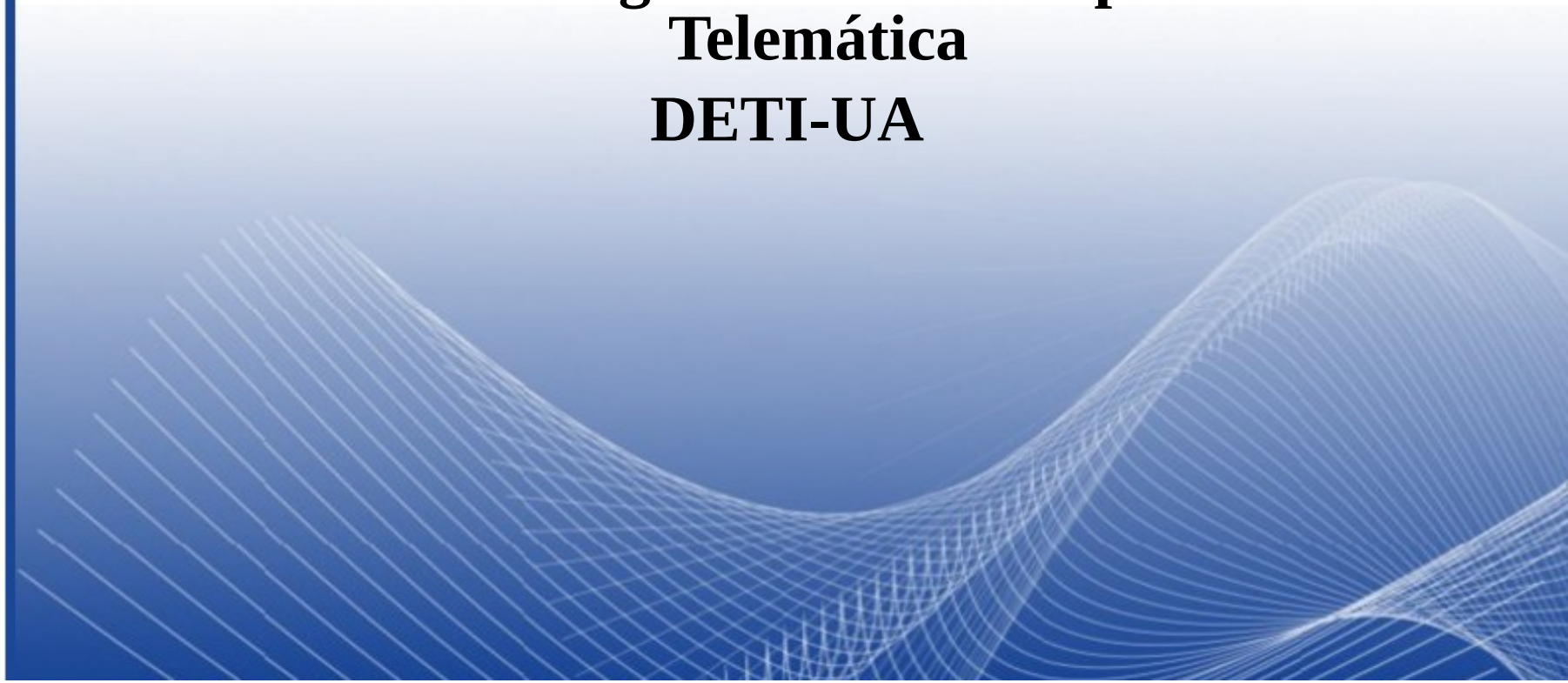
Network Access Control

Segurança em Redes de Comunicações

Mestrado em Cibersegurança

Mestrado em Engenharia de Computadores e Telemática

DETI-UA

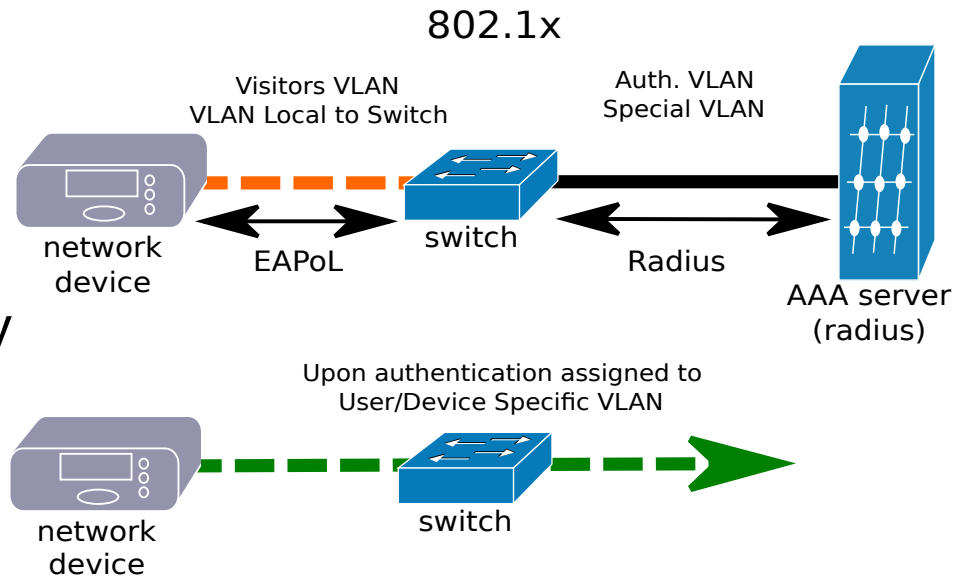


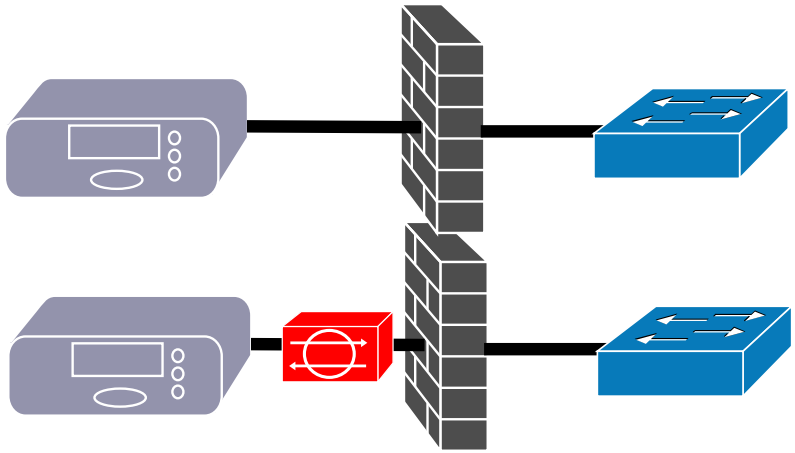
universidade de aveiro

deti.ua.pt

Illicit usage of Ethernet ports

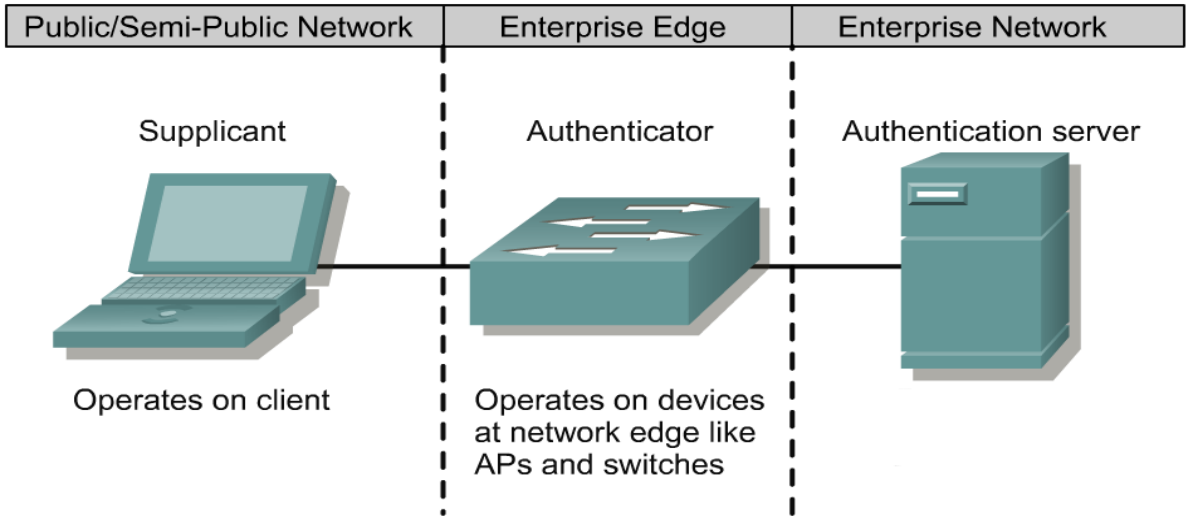
- Common protection:
  - VLAN separation/isolation.
  - 802.1X.
- Unused ports
  - VLAN separation/isolation and/or 802.1x may be enough to mitigate more dangerous attacks (L2 or L3 access to internal machines).
  - Switches MAC flooding attacks and Network overload (Local DoS) are possible.
- In use ports
  - Using an inline device it is possible to break 802.1X using terminal/user authentication.
    - Traffic pass-through.
    - After 802.1X authentication performs inline MAC spoofing.
  - Allows for traffic snooping, injection, and MITM attacks.





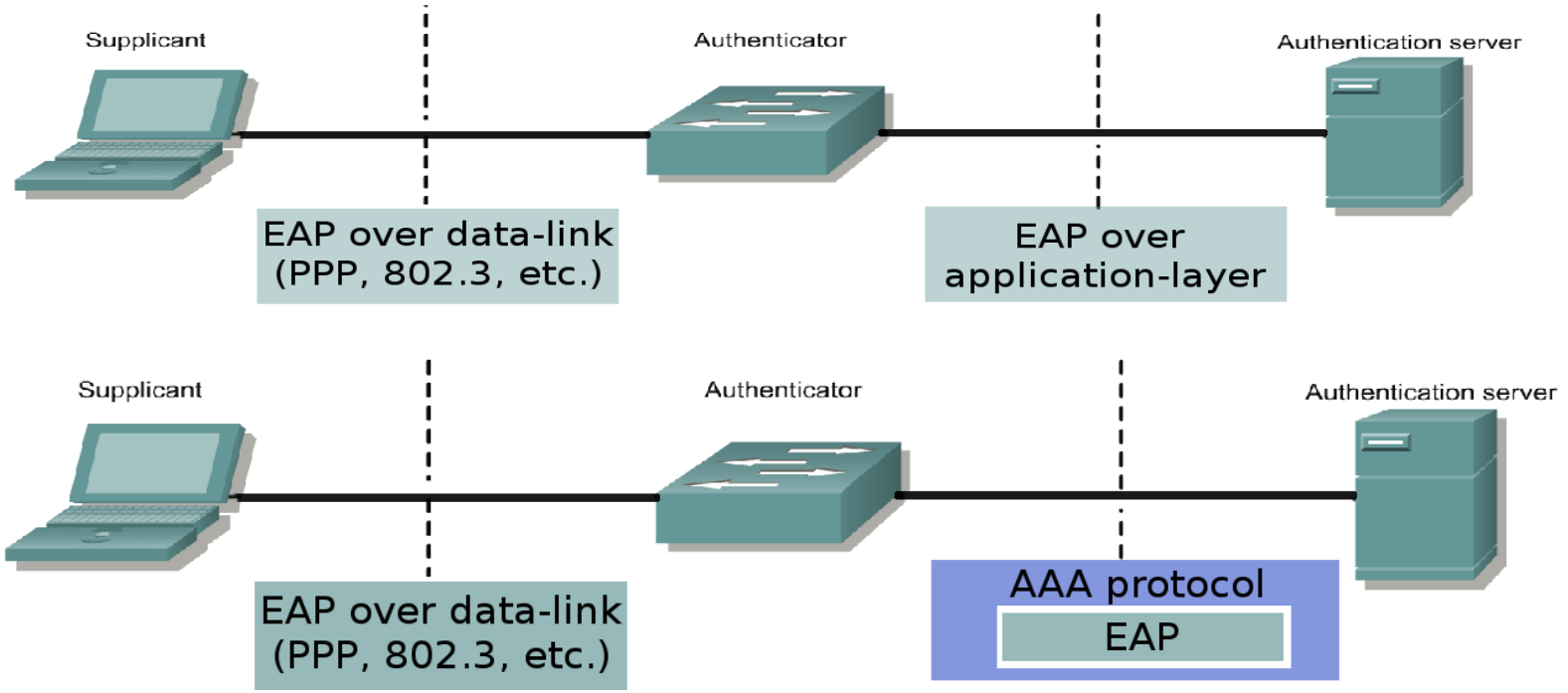
AAA Architecture

- Enables systematic access security
  - Authentication identifies an user
  - Authorization determines what that user can do
  - Accounting monitors the network usage time for billing purposes
- AAA information is typically stored in an external database or remote authentication server
- Traditional AAA Implementation



802.1X

- IEEE 802.1X is an IEEE Standard for Network Access Control (NAC)
  - 802.1X-2001 and 802.1X-2004 only provide authentication.
  - 802.1X-2010 adds optional encryption over the LAN segment.
- It provides an authentication mechanism to devices wishing to attach to a LAN.
- Based on the Extensible Authentication Protocol (EAP).
- AAA protocols/services: TACACS+, RADIUS and DIAMETER.



Extensible Authentication Protocol (EAP)

- EAP defined in [RFC3748] was designed to enable extensible authentication for network access in situations in which the Internet Protocol (IP) protocol is not available.
  - Originally developed for use with Point-to-Point Protocol (PPP) [RFC1661]
  - Subsequently also been applied to IEEE 802 wired networks [IEEE-802.1X], Internet Key Exchange Protocol version 2 (IKEv2)[RFC4306], and wireless networks such as [IEEE-802.11] and [IEEE-802.16e].
- EAP is a two-party protocol spoken between the EAP peer and server.
  - Keying material is generated by EAP authentication algorithms, known as "methods".
  - Part of this keying material can be used by EAP methods themselves, and part of this material can be exported.

EAP Overview (1)

- Where EAP key derivation is supported, the conversation typically takes place in three phases:
- Phase 0: Discovery
- Phase 1: Authentication
  - 1a: EAP authentication
  - 1b: AAA Key Transport (optional)
- Phase 2: Secure Association Protocol
  - 2a: Unicast Secure Association
  - 2b: Multicast Secure Association (optional)

EAP Overview (2)

- EAP lower layers implement phase 0, 2a, and 2b in different ways:
  - IEEE 802.1X
    - IEEE 802.1X-2004 does not support discovery (phase 0), nor does it provide for derivation of unicast or multicast secure associations (phase 2).
  - IEEE 802.11
    - Handles discovery via the Beacon and Probe Request/Response mechanisms.
    - Access Points (APs) periodically announce their Service Set Identifiers (SSIDs) as well as capabilities using Beacon frames.
    - Stations can query for APs by sending a Probe Request.
      - Neither Beacon nor Probe Request/Response frames are secured.
    - A 4-way handshake enables the derivation of unicast (phase 2a) and multicast/broadcast (phase 2b) secure associations.

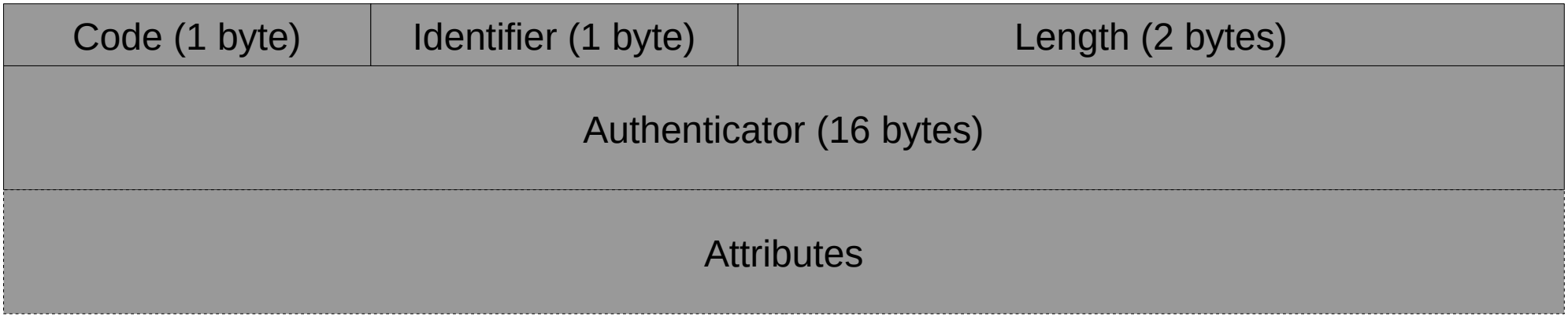
TACACS+

- Terminal Access Controller Access Control System Plus
- Forwards username and password information to a centralized security server
- Centralized server can be either a TACACS database or a database like the UNIX password le with TACACS support
- Features
  - Separates all AAA functionalities
  - Uses TCP
  - Bidirectional authentication
  - All packet is encrypted
  - Limited accounting customization

RADIUS

- Remote Authentication Dial-In User Service
- The network access device operates as a client of RADIUS
- RADIUS servers are responsible for
  - Receiving user connection requests
  - Authenticating the user
  - Return all configuration information necessary for the client to deliver service to the user
- Transactions between the client and RADIUS server are authenticated using a shared secret
- Supports a variety of methods to authenticate a user
  - PAP, CHAP, or MS-CHAP, UNIX login, and other authentication mechanisms
- Combines Authentication and Authorization. Separates Accounting (less flexible than TACACS+)
- Uses UDP (less robust)
- Unidirectional authentication
- Only encrypts the password (less secure)
- RADIUS accounting can hold more information

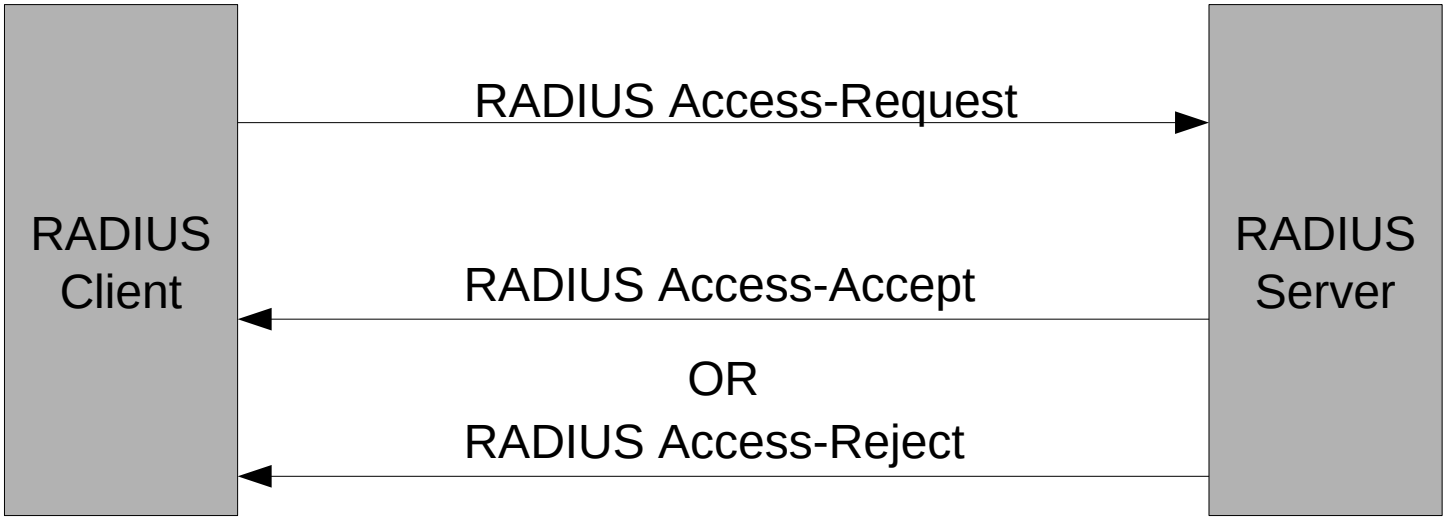
RADIUS Packet



- Code - Identifies the type of RADIUS packet
  - (1) Access-Request, (2) Access-Accept, (3) Access-Reject, (4) Accounting-Request, (5) Accounting-Response and (11) Access-Challenge
- Identifier - Allows the RADIUS client to match a RADIUS response with the correct pending request (usually is implemented as a counter)
- Authenticator
  - In client Requests – Random value
  - In server Responses - MD5 Hash function of (Code,ID,Length,Request Auth,Attributes,Shared Secret)
- Attributes - Section where an arbitrary number of attribute fields can be sent (e.g. User-Name and User-Password attributes)

RADIUS Protocol (1)

Example - RADIUS exchange involving just a username and user password:



- Only password is encrypted
  - The shared secret followed by the Request Authenticator is put through an MD5 hash to create a 16 octet value which is XORed with the password entered by the user
  - If the user password is greater than 16 octets, the password is broken into 16-octet blocks and additional MD5 calculations are performed

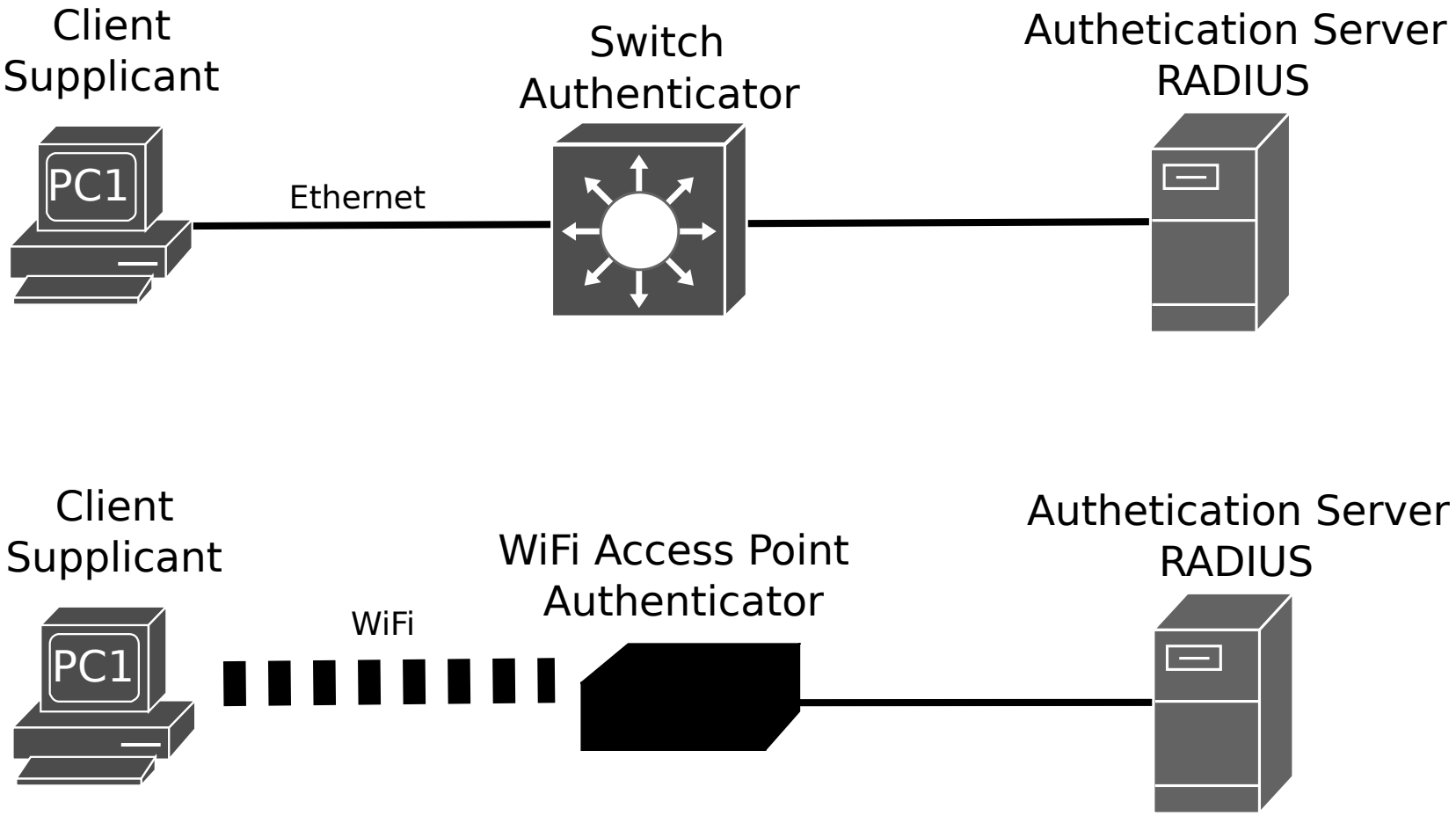
RADIUS Protocol (2)

- The RADIUS protocol has a set of vulnerabilities
  - The Access-Request packet is not authenticated at all.
  - Many client implementations do not create Request Authenticators that are sufficiently random.
  - Many administrators choose RADIUS shared secrets with insufficient information entropy and many implementations limit the shared secret key space.

DIAMETER

- DIAMETER is a newest framework in IETF for the next-generation AAA server
- Provides an AAA framework for Mobile-IP
- Does not use the same RADIUS protocol data unit, but is backward compatible with RADIUS to ease migration
- Bidirectional authentication
- It uses UDP but has a scheme that regulates the flow of packets
- Challenge/response attributes can be secured using end-to-end encryption and authentication
- Supports end-to-end security

802.1X - Ethernet vs. WiFi



Ethernet - EAP and RADIUS

11.564981	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	EAP	60	Request, Identity
11.565227	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	EAP	60	Response, Identity
11.585255	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
11.585554	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	EAP	60	Response, Legacy Nak (Response Only)
11.605541	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	EAP	60	Request, Protected EAP (EAP-PEAP)
11.606107	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	TLSv1	221	Client Hello
11.625805	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	EAP	1022	Request, Protected EAP (EAP-PEAP)
11.626628	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	EAP	60	Response, Protected EAP (EAP-PEAP)
11.646176	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	TLSv1	212	Server Hello, Certificate, Server Key Exchange, Server Hello Don
11.649978	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	TLSv1	162	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mes
11.666300	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	TLSv1	83	Change Cipher Spec, Encrypted Handshake Message
11.666636	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	EAP	60	Response, Protected EAP (EAP-PEAP)
11.686625	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	TLSv1	61	Application Data
11.686915	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	TLSv1	98	Application Data, Application Data
11.706925	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	TLSv1	93	Application Data
11.708108	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	TLSv1	162	Application Data, Application Data
11.727323	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	TLSv1	109	Application Data
11.728248	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	TLSv1	98	Application Data, Application Data
11.747691	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	TLSv1	61	Application Data
11.748540	PcsCompu_64:26:6d	Nearest-non-TPMR-bridge	TLSv1	98	Application Data, Application Data
11.768072	c2:01:d1:5d:f1:00	PcsCompu_64:26:6d	EAP	60	Success

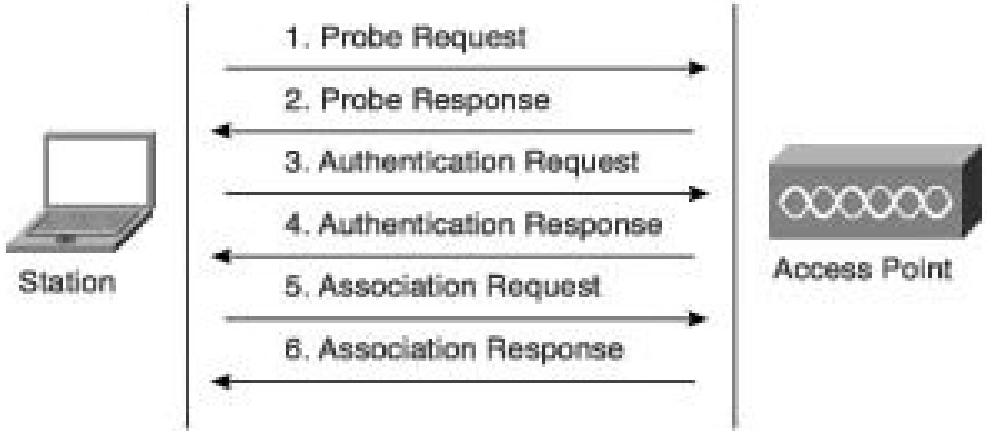
0.000000	10.0.0.1	10.0.0.100	RADIUS	154	Access-Request id=1
0.000594	10.0.0.100	10.0.0.1	RADIUS	122	Access-Challenge id=1
0.020271	10.0.0.1	10.0.0.100	RADIUS	165	Access-Request id=2
0.020944	10.0.0.100	10.0.0.1	RADIUS	106	Access-Challenge id=2
0.040451	10.0.0.1	10.0.0.100	RADIUS	362	Access-Request id=3
0.049097	10.0.0.100	10.0.0.1	RADIUS	1110	Access-Challenge id=3
0.060742	10.0.0.1	10.0.0.100	RADIUS	165	Access-Request id=4
0.062137	10.0.0.100	10.0.0.1	RADIUS	294	Access-Challenge id=4
0.081103	10.0.0.1	10.0.0.100	RADIUS	303	Access-Request id=5
0.081845	10.0.0.100	10.0.0.1	RADIUS	165	Access-Challenge id=5
0.101366	10.0.0.1	10.0.0.100	RADIUS	165	Access-Request id=6
0.101883	10.0.0.100	10.0.0.1	RADIUS	143	Access-Challenge id=6
0.121651	10.0.0.1	10.0.0.100	RADIUS	239	Access-Request id=7
0.122255	10.0.0.100	10.0.0.1	RADIUS	175	Access-Challenge id=7
0.141930	10.0.0.1	10.0.0.100	RADIUS	303	Access-Request id=8
0.143019	10.0.0.100	10.0.0.1	RADIUS	191	Access-Challenge id=8
0.162277	10.0.0.1	10.0.0.100	RADIUS	239	Access-Request id=9
0.163695	10.0.0.100	10.0.0.1	RADIUS	143	Access-Challenge id=9
0.182642	10.0.0.1	10.0.0.100	RADIUS	239	Access-Request id=10
0.184255	10.0.0.100	10.0.0.1	RADIUS	212	Access-Accept id=10

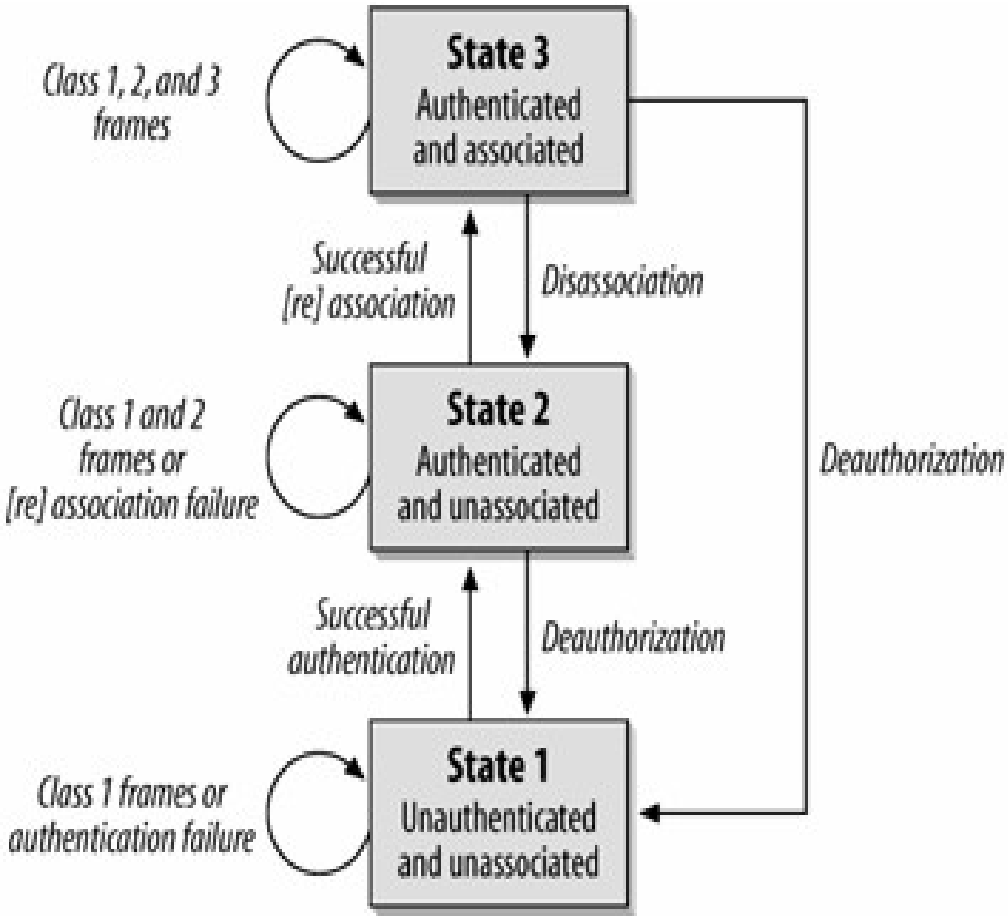
IEEE 802.11 services

- Station services (similar to wired network)
  - Authentication (login)
  - De-authentication (logout)
  - Privacy
  - Data delivery
- Distribution services
  - Association
    - Make logical connection between the AP and the station – the AP will not receive any data from a station before association
  - Re-association (similar to association)
    - Send repeatedly to the AP.
    - Help the AP to know if the station has moved from/to another BSS.
    - After Power Save
  - Disassociation
    - Manually disconnect (PC is shutdown or adapter is ejected)

Joining a BSS

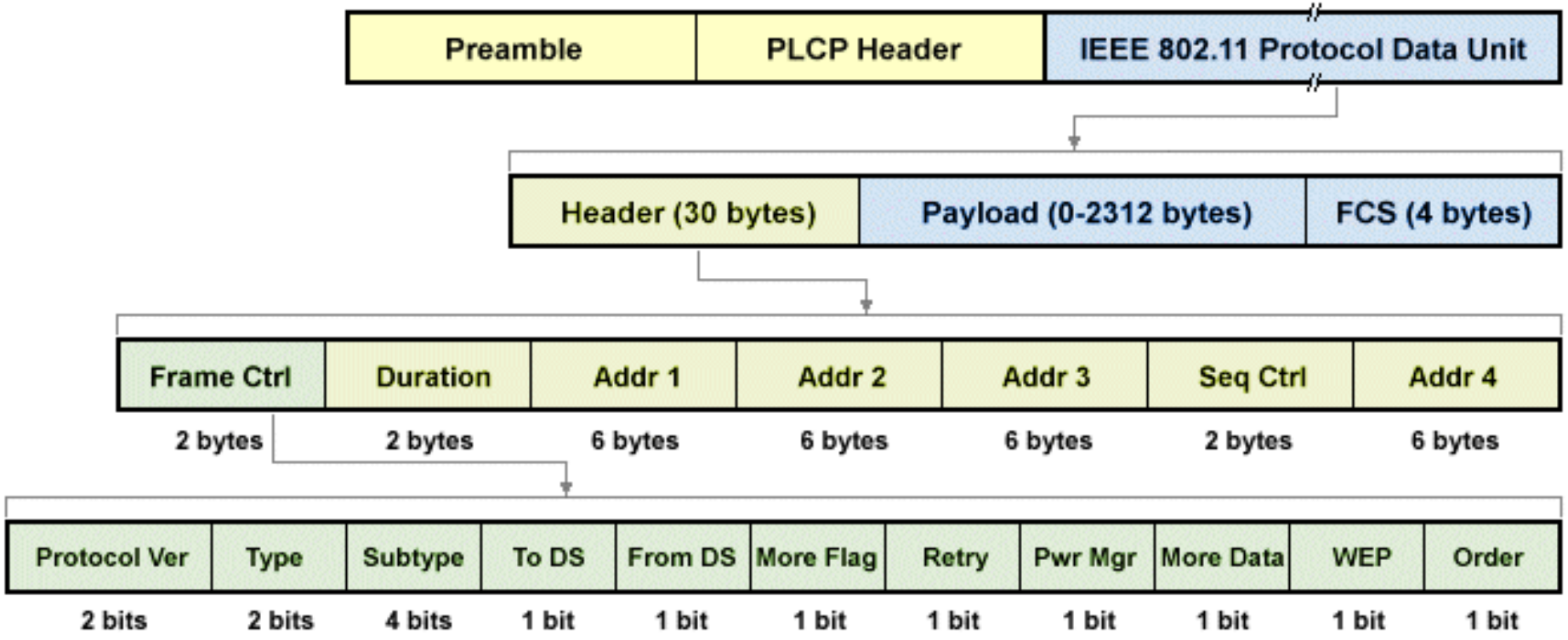
- Station finds BSS/AP by **Scanning/Probing**.
- BSS with AP: both **Authentication** and **Association** are necessary for joining a BSS.





WLAN Frames

- Three types of frames
  - Control: RTS, CTS, ACK
  - Management
  - Data
- Header is different for the different types of frames.



Joining BSS with AP: Scanning

- A station willing to join a BSS must get in contact with the AP. This can happen through:
- 1. Passive scanning
  - The station scans the channels for a Beacon frame that is sent periodically from an AP to announce its presence and provide the SSID, and other parameters for WNICs within range
- 2. Active scanning (the station tries to find an AP)
  - The station sends a Probe Request frame - Sent from a station when it requires information from another station
  - All AP's within reach reply with a Probe Response frame - Sent from an AP containing capability information, supported data rates, etc., after receiving a probe request frame

Beacon Frame

```
▾ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ▸ Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    .... .... .... 0000 = Fragment number: 0
    1001 1000 1010 .... = Sequence number: 2442
    Frame check sequence: 0x6f0b825c [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (12 bytes)
      Timestamp: 660070796
      Beacon Interval: 0.102400 [Seconds]
    ▸ Capabilities Information: 0x0421
  ▾ Tagged parameters (123 bytes)
    ▸ Tag: SSID parameter set: LABCOM
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 13
    ▸ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▸ Tag: ERP Information
    ▸ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▸ Tag: Cisco CCX1 CKIP + Device Name
    ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (1) (1)
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet CCX version = 5
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (11) (11)
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Client MFP Disabled
```

Probe Request/Response Frames

```
IEEE 802.11 Probe Request, Flags: ........C
  Type/Subtype: Probe Request (0x0004)
  Frame Control Field: 0x4000
  .000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  Transmitter address: Microsof_0a:43:e3 (c0:33:5e:0a:43:e3)
  Source address: Microsof_0a:43:e3 (c0:33:5e:0a:43:e3)
  BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
  .... .... .... 0000 = Fragment number: 0
  1100 1011 0001 .... = Sequence number: 3249
  Frame check sequence: 0xc7056d0a [unverified]
  [FCS Status: Unverified]
IEEE 802.11 wireless LAN
  Tagged parameters (62 bytes)
    Tag: SSID parameter set: TD_WIFI_GUEST
    Tag: Supported Rates 1, 2, 5.5, 6, 9, 11, 12, 18, [Mbit/sec]
    Tag: DS Parameter set: Current Channel: 13
    Tag: HT Capabilities (802.11n D1.10)
    Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
```

```
IEEE 802.11 Probe Response, Flags: ........C
  Type/Subtype: Probe Response (0x0005)
  Frame Control Field: 0x5000
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: IntelCor_d2:98:58 (28:b2:bd:d2:98:58)
  Destination address: IntelCor_d2:98:58 (28:b2:bd:d2:98:58)
  Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  .... .... .... 0000 = Fragment number: 0
  1010 0010 1001 .... = Sequence number: 2601
  Frame check sequence: 0x80831320 [unverified]
  [FCS Status: Unverified]
IEEE 802.11 wireless LAN
  Fixed parameters (12 bytes)
    Timestamp: 664064263
    Beacon Interval: 0.102400 [Seconds]
    Capabilities Information: 0x0421
  Tagged parameters (117 bytes)
    Tag: SSID parameter set: LABCOM
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
    Tag: DS Parameter set: Current Channel: 13
    Tag: ERP Information
    Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    Tag: Cisco CCX1 CKIP + Device Name
    Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (1) (1)
    Tag: Vendor Specific: Cisco Systems, Inc.: Aironet CCX version = 5
    Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (11) (11)
    Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Client MFP Disabled
```

Joining BSS with AP: Authentication

- Once an AP is found/selected, a station goes through authentication
- Open system authentication (default, 2-step process)
  - Station sends authentication frame with its identity
  - AP sends frame as an Ack / NAck
- Shared key authentication
  - Stations receive shared secret key through secure channel independent of 802.11
  - After the WNIC sends its initial authentication request, it will receive an authentication frame from the AP containing a challenge text
  - The WNIC sends an authentication frame containing the encrypted version of the challenge text to the AP.
  - The AP ensures the text was encrypted with the correct key by decrypting it with its own key.
  - The result of this process determines the WNIC's authentication status.

Authentication Frames

- Nowadays, WPA* sedcure networks use “Open System”.
- Non-”Open System” authentication was used for WEP protected networks (unsecured and functionally deprecated).

```
IEEE 802.11 Authentication, Flags: ........
  Type/Subtype: Authentication (0x000b)
  Frame Control Field: 0xb000
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Destination address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Transmitter address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Source address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  .... .... .... 0000 = Fragment number: 0
  0001 0100 1011 .... = Sequence number: 331
IEEE 802.11 wireless LAN
  Fixed parameters (6 bytes)
    Authentication Algorithm: Open System (0)
    Authentication SEQ: 0x0001
    Status code: Successful (0x0000)
```

← From Station

From AP →

```
IEEE 802.11 Authentication, Flags: ........C
  Type/Subtype: Authentication (0x000b)
  Frame Control Field: 0xb000
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  .... .... .... 0000 = Fragment number: 0
  1010 1001 0000 .... = Sequence number: 2704
  Frame check sequence: 0x9f8350e1 [unverified]
  [FCS Status: Unverified]
IEEE 802.11 wireless LAN
  Fixed parameters (6 bytes)
    Authentication Algorithm: Open System (0)
    Authentication SEQ: 0x0002
    Status code: Successful (0x0000)
```

Joining BSS with AP: Association

- Once a station is authenticated, it starts the association process, i.e., information exchange about the AP/station capabilities and roaming
  - STA → AP: Associate Request frame
    - Enables the AP to allocate resources and synchronize. The frame carries information about the WNIC, including supported data rates and the SSID of the network the station wishes to associate with.
  - AP → STA: Association Response frame
    - Acceptance or rejection to an association request. If it is an acceptance, the frame will contain information such as association ID and supported data rates.
  - New AP informs old AP (if it is a handover).
- Only after association is completed, a station can transmit and receive data frames.

Association Request/Response Frames

← From Station

```
IEEE 802.11 Association Request, Flags: ........
  Type/Subtype: Association Request (0x0000)
  Frame Control Field: 0x0000
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Destination address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Transmitter address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Source address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  .... .... .... 0000 = Fragment number: 0
  0001 0100 1100 .... = Sequence number: 332
IEEE 802.11 wireless LAN
  Fixed parameters (4 bytes)
    Capabilities Information: 0x0421
    Listen Interval: 0x000a
  Tagged parameters (43 bytes)
    Tag: SSID parameter set: LABCOM
    Tag: Supported Rates 1, 2, 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
    Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    Tag: Extended Capabilities (8 octets)
    Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information E
```

From AP →

```
IEEE 802.11 Association Response, Flags: ........C
  Type/Subtype: Association Response (0x0001)
  Frame Control Field: 0x1000
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  .... .... .... 0000 = Fragment number: 0
  1010 1001 0001 .... = Sequence number: 2705
  Frame check sequence: 0xe7103b15 [unverified]
  [FCS Status: Unverified]
IEEE 802.11 wireless LAN
  Fixed parameters (6 bytes)
    Capabilities Information: 0x0421
    Status code: Successful (0x0000)
    ..00 0000 0000 0001 = Association ID: 0x0001
  Tagged parameters (42 bytes)
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
    Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

Data Frame

```
▾ IEEE 802.11 QoS Data, Flags: .p.....TC
    Type/Subtype: QoS Data (0x0028)
  ▸ Frame Control Field: 0x8841
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
    Transmitter address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
    Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
    Source address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
    BSS Id: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
    STA address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
    .... .... .... 0000 = Fragment number: 0
    0000 0000 0011 .... = Sequence number: 3
    Frame check sequence: 0xc72771e8 [unverified]
    [FCS Status: Unverified]
  ▸ Qos Control: 0x0000
  ▸ CCMP parameters
▾ Data (1244 bytes)
    Data: f8002648417037bc923106ead1717d4821fde0989beb08b1…
    [Length: 1244]
```

← Node that will receive frame (AP)
← Node that send frame
← Station to receive data
← Station who sent data

- Station “IntelCor*” sending data to station “D-LinkIn*” (via AP).
- Frame captured between station “IntelCor*” and AP (“Cisco*”).

WPA and 802.11i (WPA2)

- **IEEE 802.11i - IEEE 802.11 task group “MAC enhancement for wireless security”.**
- **Wi-Fi Protected Access (WiFi Alliance), WPA, is a subset internal in 802.11i.**
  - Compatible with work developed in 802.11i.
  - Only supports BSS.
  - Defined to work in actual equipment.
    - Firmware update only.
  - Pass-phrase constant and shared, but keys are generated per session.
  - Used in the AP and station.
- WPA has two distinct components.
  - Authentication, based on 802.1X.
  - Ciphering based on TKIP (Temporal Key Integrity Protocol).

WPA

- Authentication
  - 802.1X (≠ 802.11x) – defined for wired and wireless sessions, as a transport protocol
    - EAP (Extensible Authentication Protocol) – like a wrapper for the specific authentication traffic
    - Impact of EAP
      - Authentication does not traverse the AP (STA - server)
      - It is possible to use different authentication methods without changing APs
  - Defines also a Pre-Shared Key (PSK)
    - For local networks
- Temporal Key Integrity Protocol (TKIP) – internal solution with better protection, for actual equipments
  - Greater privacy
    - Uses the same cipher, but now associated to the MAC and a larger IV
    - “Key rollover” with temporal validity
  - Greater integrity
    - Integrity separated key

802.11i (WPA2)

- Better than WPA
  - Also includes TKIP
  - Authentication IBSS (ad-hoc mode)?
  - RSN (Robust Security Network) protocol
    - Authentication and ciphering between APs and stations
    - Supports new ciphering protocols, resorting to 802.1x and EAP
    - Supports AES (Advanced Encryption Standard) ciphering
- Problems
  - It does not cipher control and management frames
    - (Disassociate, output power, etc).
  - Requires new hardware

WPA* Key Exchange (EAP phase 2)

- Done during the Association process.
  - After Association Request/response frames.
  - Uses (QoS) Data Frames

```
  205 595.669409767  IntelCor_e8:14:53    Cisco_61:ee:d1         802.11   110 Association Request, SN=38, FN=0, Flags=........, SSID=LABCOM_SEC
  206 595.671214291  Cisco_61:ee:d1       IntelCor_e8:14:53      802.11   128 Association Response, SN=14, FN=0, Flags=........
  207 595.673042781  Cisco_61:ee:d1       IntelCor_e8:14:53      EAPOL    211 Key (Message 1 of 4)
  208 595.678333124  IntelCor_e8:14:53    Cisco_61:ee:d1         EAPOL    168 Key (Message 2 of 4)
  209 595.681795313  Cisco_61:ee:d1       IntelCor_e8:14:53      EAPOL    269 Key (Message 3 of 4)
  210 595.683690439  IntelCor_e8:14:53    Cisco_61:ee:d1         EAPOL    146 Key (Message 4 of 4)
```

```
▸ Frame 207: 211 bytes on wire (1688 bits), 211 bytes captured (1688 bits) on interface 0
▸ Radiotap Header v0, Length 56
▸ 802.11 radio information
▾ IEEE 802.11 QoS Data, Flags: ......F.
    Type/Subtype: QoS Data (0x0028)
  ▸ Frame Control Field: 0x8802
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
    Transmitter address: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
    Destination address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
    Source address: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
    BSS Id: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
    STA address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
    .... .... .... 0000 = Fragment number: 0
    0000 0001 1100 .... = Sequence number: 28
  ▸ Qos Control: 0x0007
▸ Logical-Link Control
▾ 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 117
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
  ▸ Key Information: 0x008a
    Key Length: 16
    Replay Counter: 1
    WPA Key Nonce: 4f65d0b4e9e77b88f2cbb135749eeb105a3aa1ef65de66a8…
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 22
  ▸ WPA Key Data: dd14000fac046616ebb59b83e8cc1816ced0e542a935
```

Extra References

- Cisco, Wired 802.1X Deployment Guide
- H. N. Thakur, A. Al Hayajneh, K. Thakur, A. Kamruzzaman and M. L. Ali, " A Comprehensive Review of Wireless Security Protocols and Encryption Applications," 2023 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 2023, pp. 0373-0379, doi: 10.1109/AIIoT58121.2023.10174571.
- M. Alhamry and A. Alomary, "Exploring Wi-Fi WPA2-PSK protocol weaknesses," 2022 International Conference on Data Analytics for Business and Industry (ICDABI), Sakhir, Bahrain, 2022, pp. 190-195, doi:10.1109/ICDABI56818.2022.10041465.

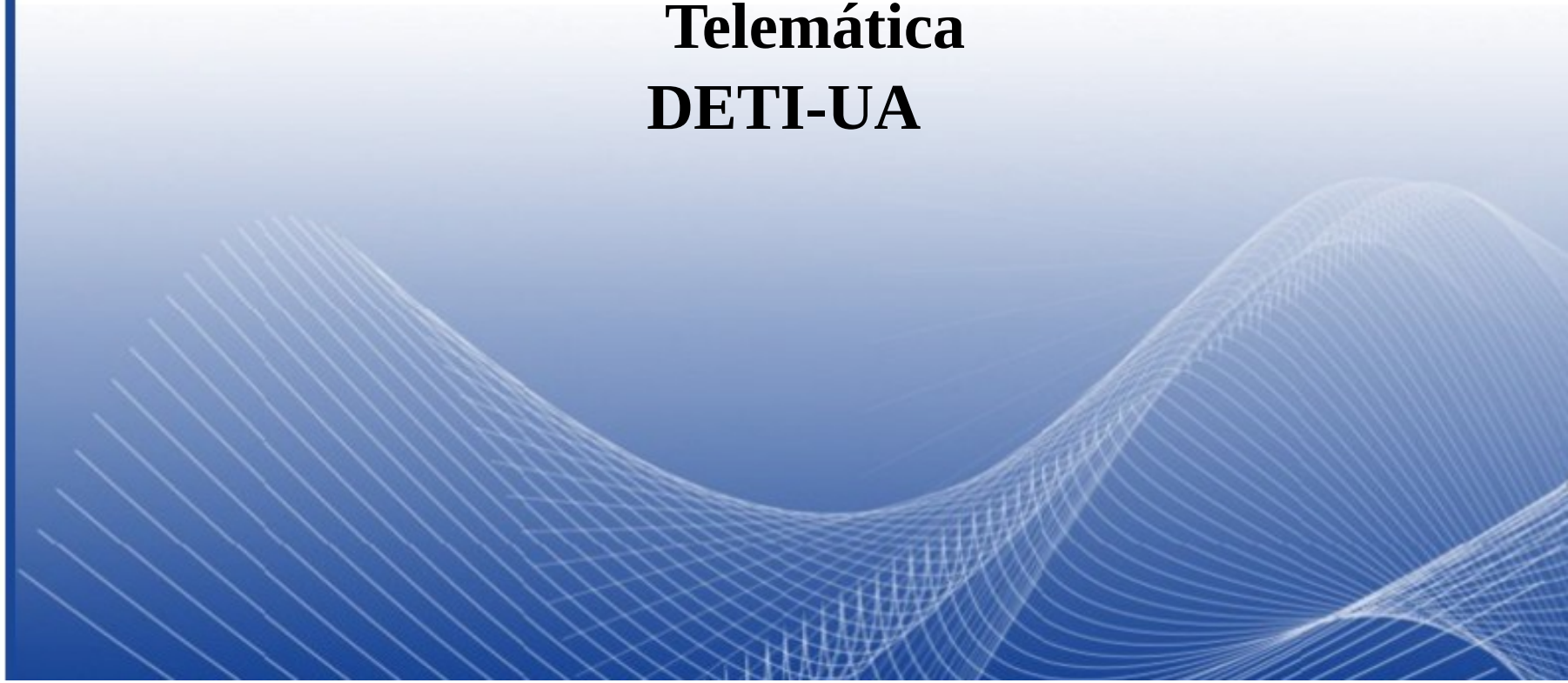
Network Flow Control

Segurança em Redes de Comunicações

Mestrado em Cibersegurança

Mestrado em Engenharia de Computadores e Telemática

DETI-UA

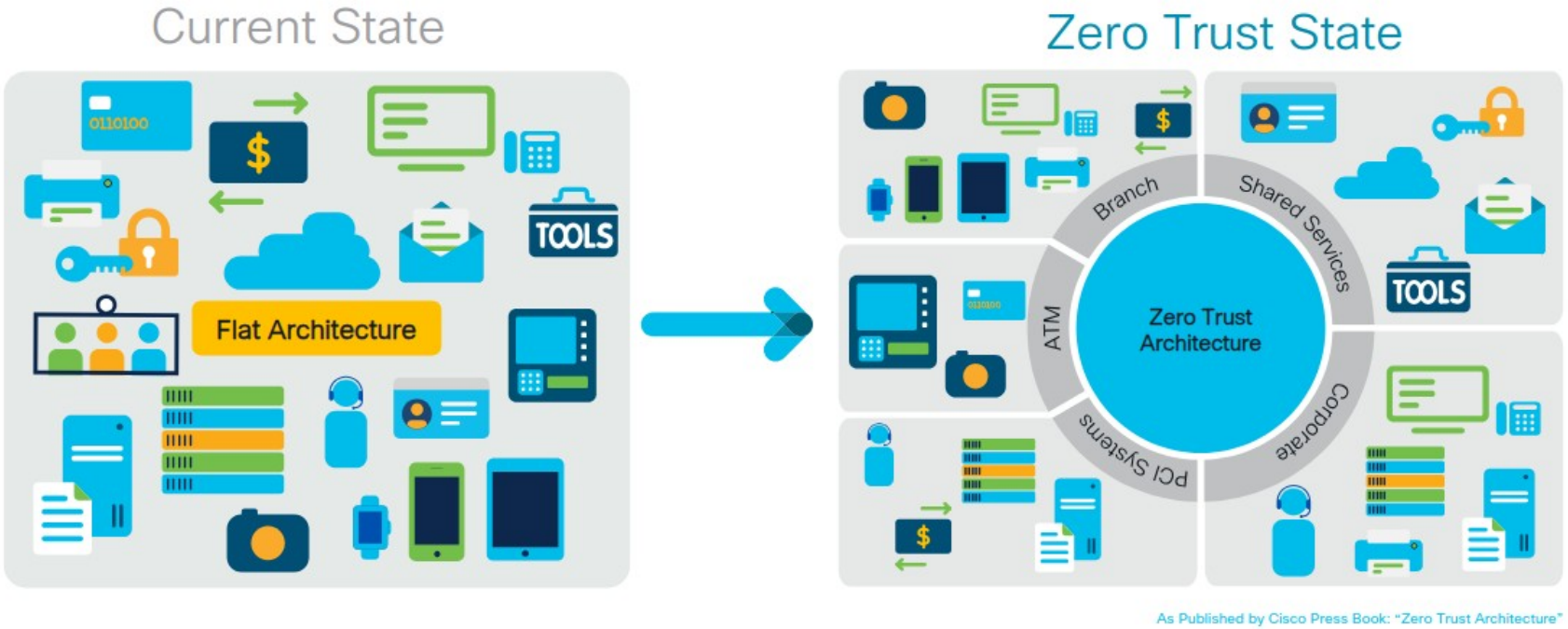


universidade de aveiro

deti.ua.pt

Network (micro-)segmentation

- One of the concepts to create a Zero Trust Architecture
- Security strategy that divides a network into smaller and isolated segments.
- Can be achieved by creating data flow boundaries and enforcing strict controls between different segments.



Firewalls

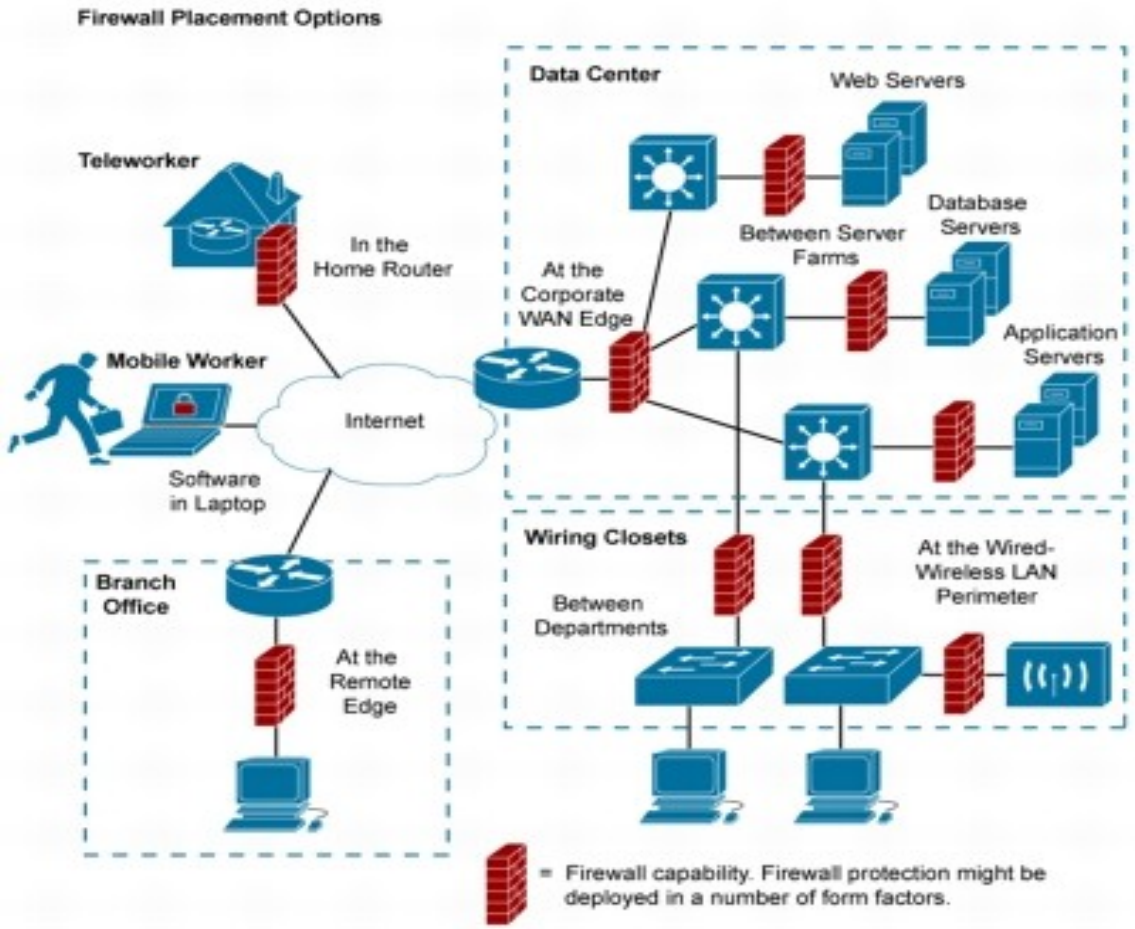
- A firewall provides a single point of defense between networks and protects one network from the others.
- It is a system or group of systems that enforces a control policy between two or more networks (access control, flow control and content control).
- It is a network gateway that enforces the rules of network security.
- Minimizes local vulnerabilities.
- Evaluates each network packet against the policies of network security.
- Can monitor all the network traffic and alert to any attempts to bypass security or to any patterns of inappropriate use.
- Can be hardware or software based.

Firewalls Security/Network Services

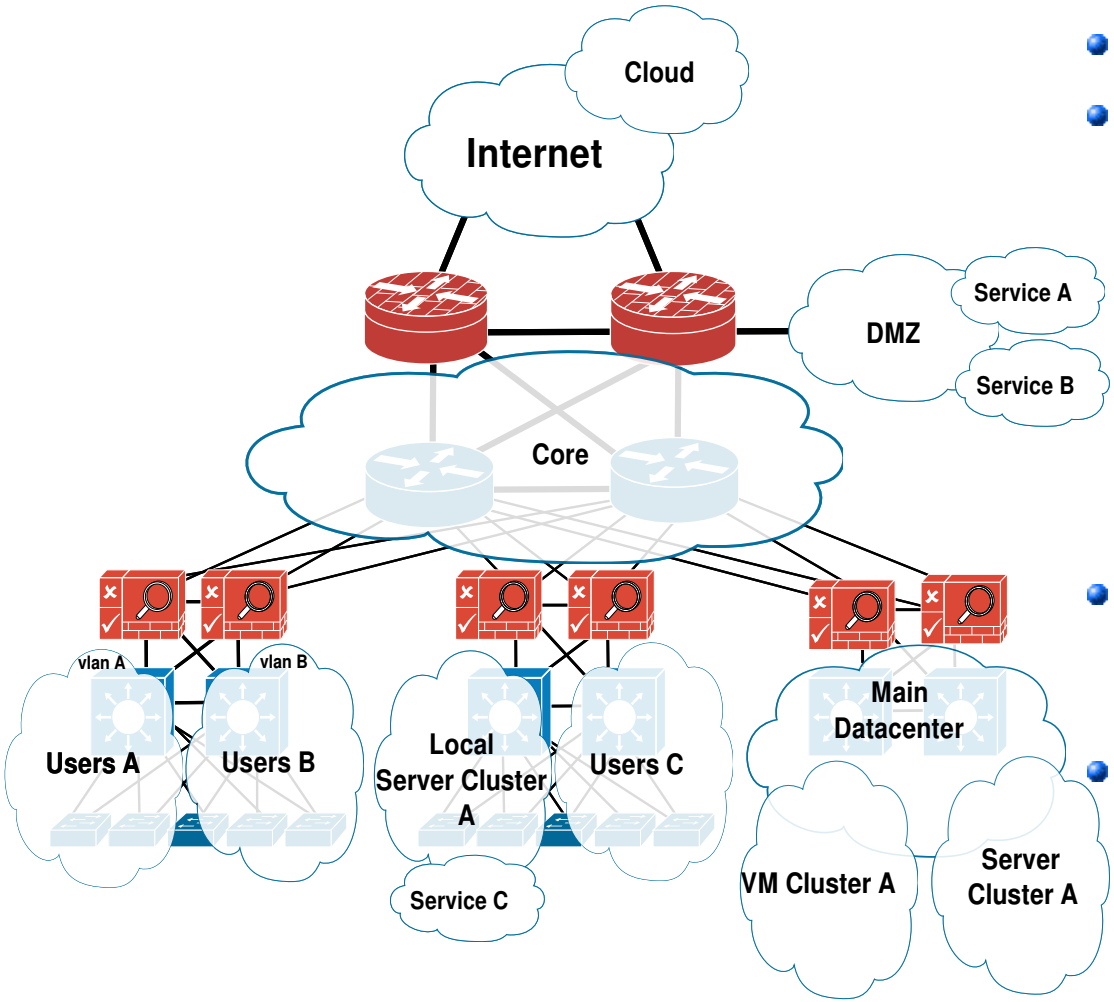
- NAT (Network Address Translation).
- Authorization
  - Flows (packet filtering).
  - Users (application and circuit level).
- Redirecting.
  - To specif machines.
  - Proxing.
- Content analysis.
- Secure communication.
  - Site-to-site VPN.
    - IPsec.
  - Remote-access VPN.
- DoS and DDoS detection and defense.

Deploying Firewalls

- Zero Trust imposes that network must have micro-segmentation.
- Network must be controlled at multiple levels and locations



Firewall Zones/Segments/Groups



- A network must be micro-segmented.
- Must be divided in multiple zones/segments/groups with different security levels.
  - Collections of network ports, IP addresses, IP networks, service ports, Security Group Tags (SGT), other IDs.
  - Some firewalls only allow zones defined by interface name. Other IDs only used to define traffic source/destination.
- Once created, a group can be referenced by firewall rules as either a source or destination.
- Example: a Demilitarized Zone (DMZ) is a perimeter network outside the protected internal/private network
  - Used to place public servers/services.
  - The DMZ is a "semi-protected" Zone.
    - It must be assumed that any machine placed on the DMZ is at risk.

Types of Firewalls

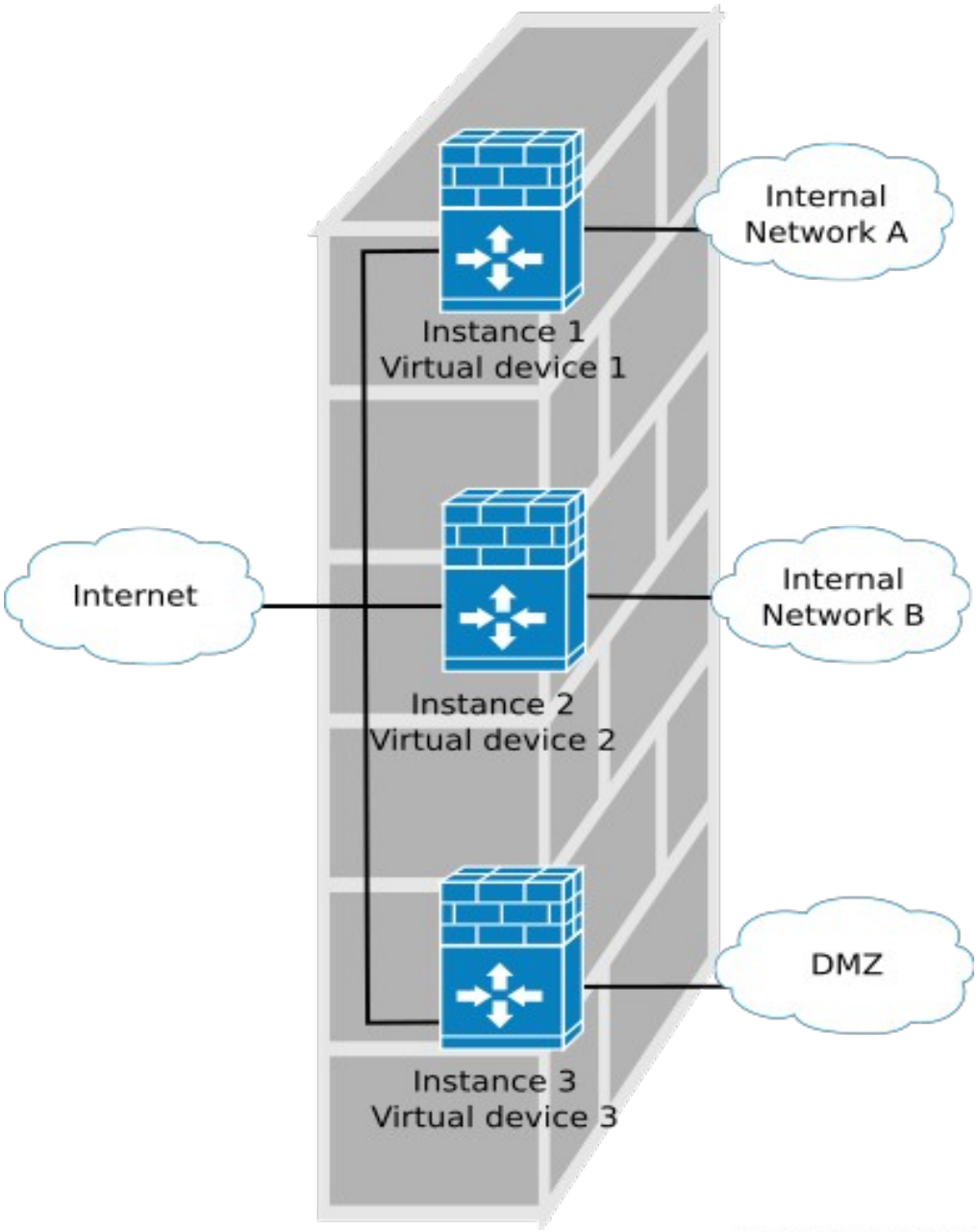
- Network-Level Firewalls (L2/L3)
  - Packet filtering
  - Inspecting packet headers and filtering traffic based on
    - the IP address of the source and the destination, the port and the service (L3)
    - source and the destination MAC addresses (L2)
- Circuit-Level Firewalls (L4)
  - Monitor TCP handshaking between packets to make sure a session is legitimate
  - Traffic is filtered based on specified session rules
- Application-Level Firewalls (L4+)
  - Application-level firewalls are sometimes called proxies
  - Looking more deeply into the application data
  - Consider the context of client requests and application responses
  - Attempt to enforce correct application behavior and block malicious activity
  - Application-level filtering may include protection against Spam and viruses as well, and block undesirable Web sites based on content rather than just their IP address
  - Slow and resources consuming tasks
- Stateful Multi-level Firewalls (L*)
  - Filter packets at the network level and they recognize and process application-level data
  - Since they don't employ proxies, they have reasonably good performance even performing deep packet analysis
- Host Level / Personal Firewalls
  - Act only within a specif host
  - Filter all communication layers
  - Control OS processes/applications

Stateful vs. Stateless Firewalls

- Stateless firewalls
  - Controls traffic by applying rules to single frames/packets
    - Does not need to track traffic flows/sessions.
  - Rules based on specific values on frames/packet available headers.
    - Set of basic permit/deny actions for input and output based on IP addresses, UDP/TCP ports, etc…
    - Usually called ACL (Access List).
  - They are fast and consume very low computing resources.
    - Perform well under heavy traffic load.
    - Ideal to defense against DDoS attacks in the first line of network defense.
    - Cost-effective compared with stateful firewall types.
- Stateful firewalls
  - Monitor all traffic flows/sessions.
  - Controls traffic based on the connection state of a flow/session.
    - Automatic bidirectional rules (reflexive rules).
  - Connection state is maintained in a state table.
    - State tables must be synchronized with other firewalls when in a redundant scenario (load balancing) or high-availability scenario (backup upon failure).

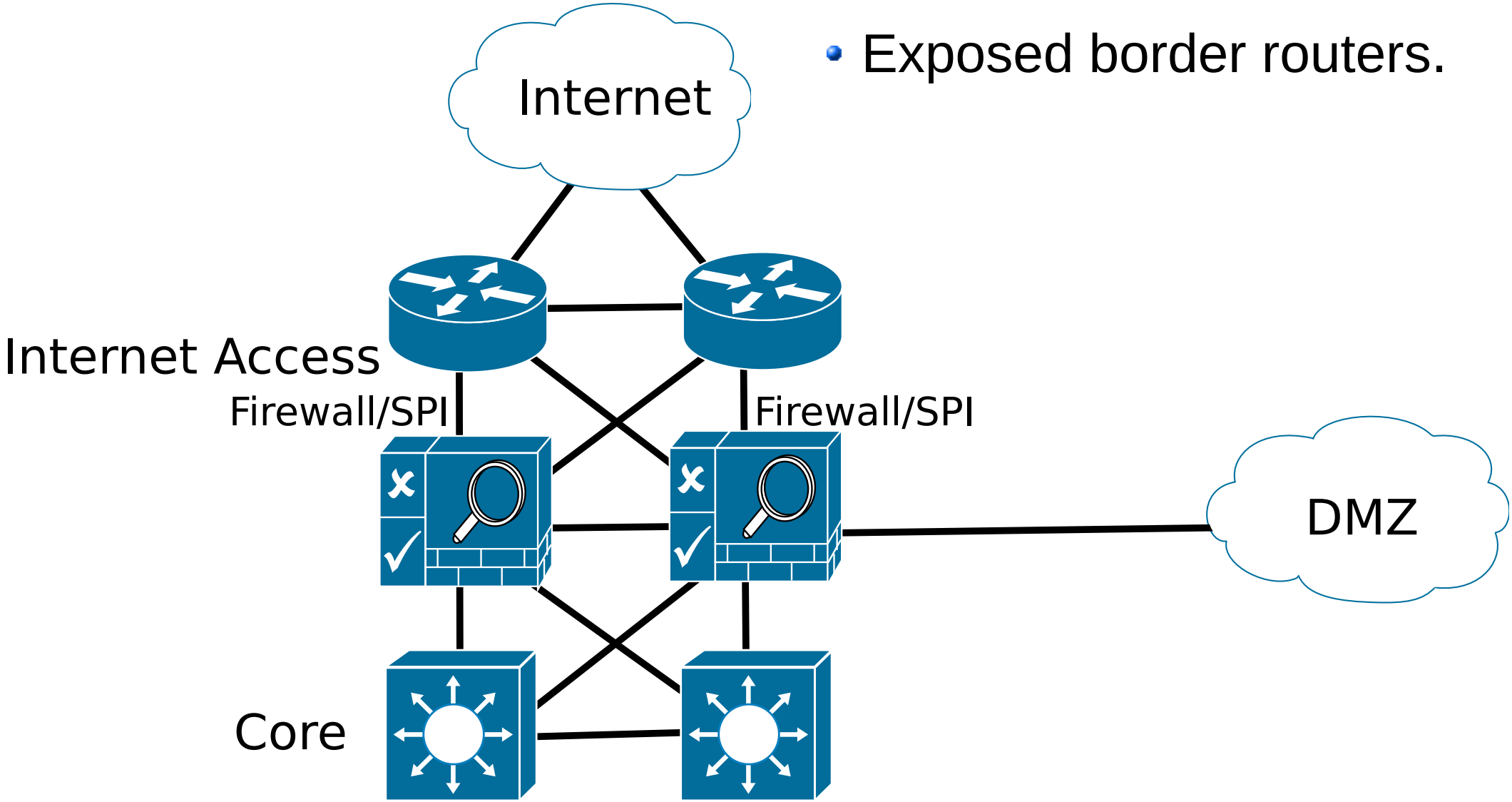
Firewall Virtual Instances

- Firewalls may have (theoretical) isolated instances to handle different zones/groups.
- Each instance is a virtual device that can perform flow control, switch, and/or routing.



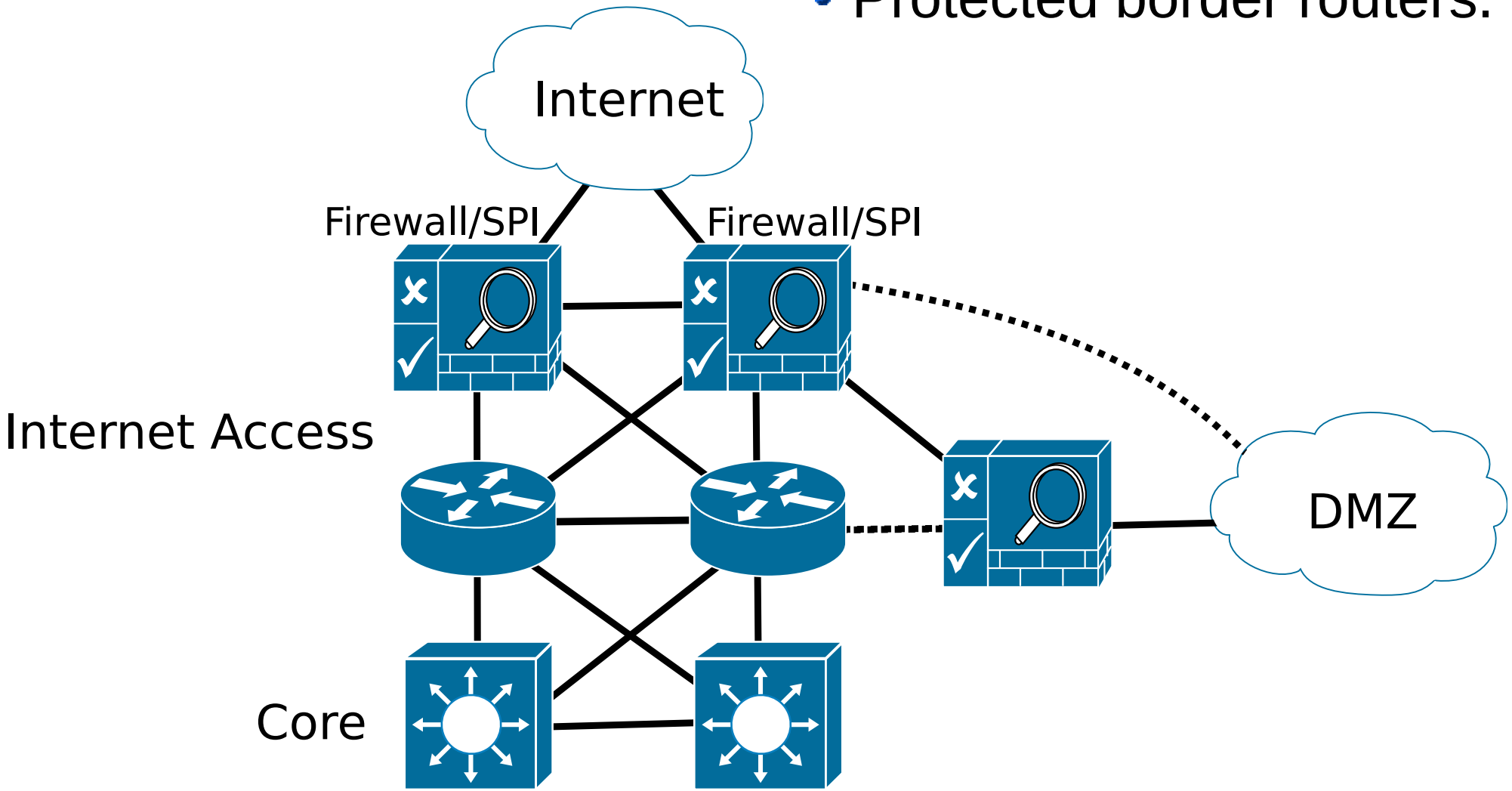
Firewall placement (with Redundancy)

- Exposed border routers.



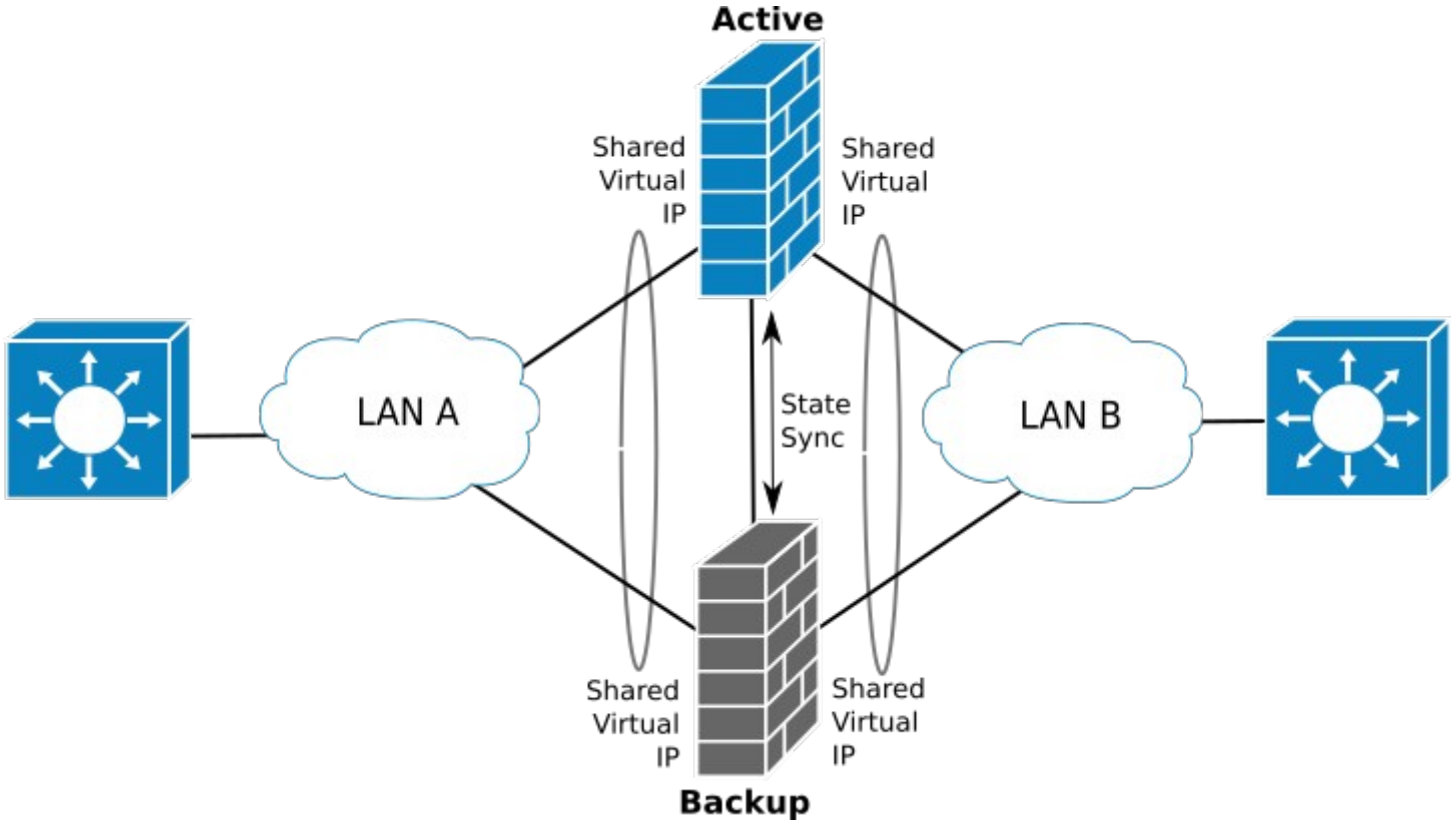
Firewall placement (with Redundancy)

- Protected border routers.



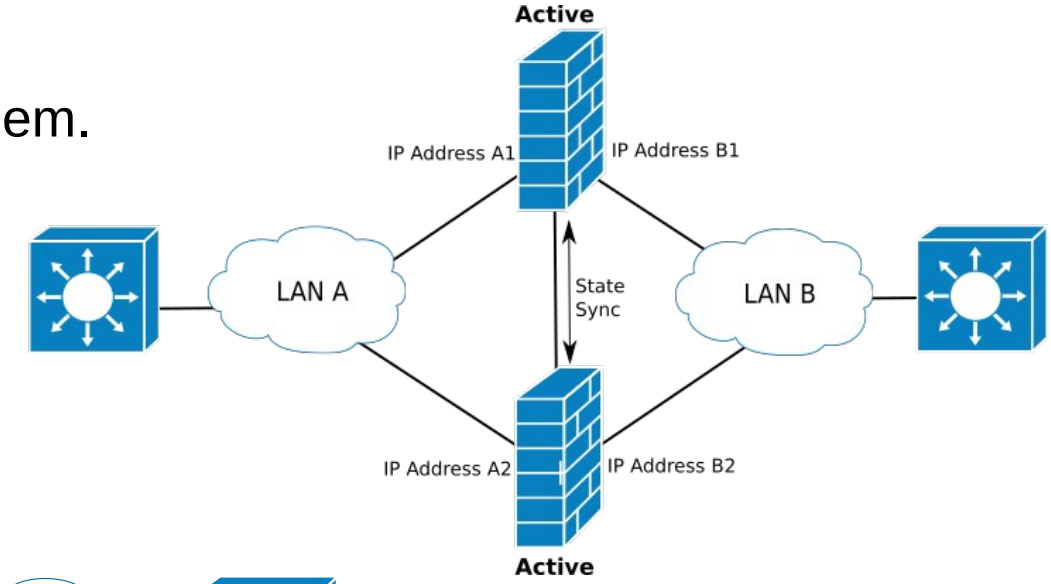
High-Availability (1)

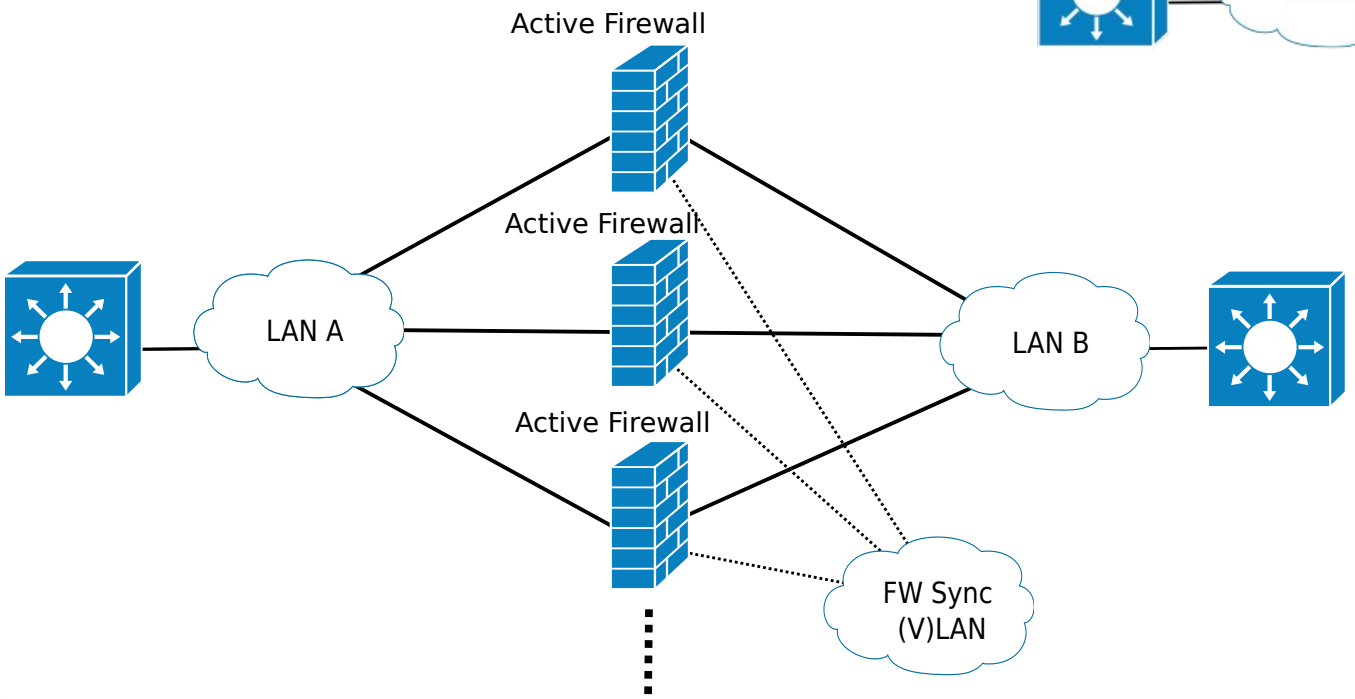
- Active-Backup Scenario
  - Firewalls share state via a dedicated connection
  - Firewalls share LAN (Virtual) IP addresses.
  - Backup firewall assumes IP and Services upon failure of Active firewall.
  - Usually implemented with Virtual Router Redundancy Protocol (VRRP)
    - FWs use the same MAC and IP addresses
    - The backup FW assumes addresses and functions upon detection of the active FW failure.



High-Availability / Cluster (2)

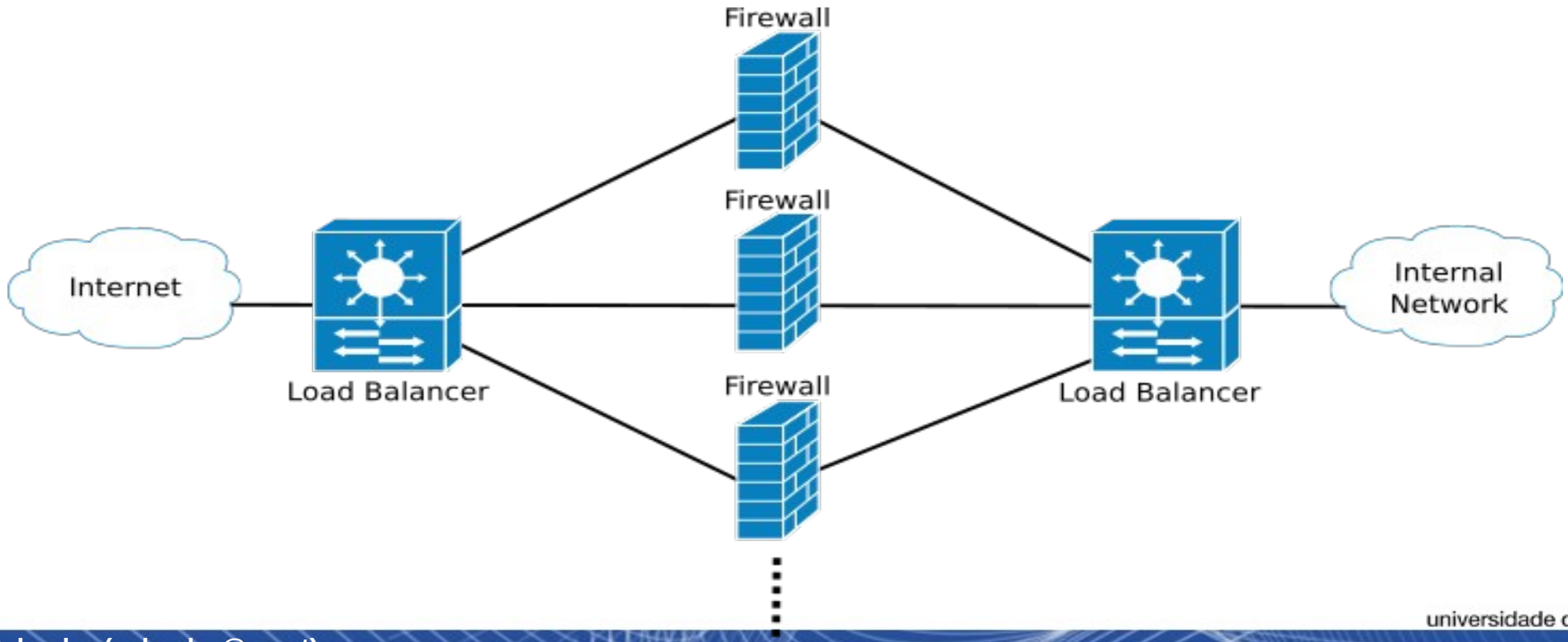
- Active-Active Scenario
  - Multiple firewalls (cluster) share state via a dedicated connection/(V)LAN
  - Firewalls have their on IP addresses.
  - Both work simultaneously.
    - Share load.
    - Solve asymmetric routing problem.
    - Work with load-balancers.





Load Balancing Firewall Load

- Load-balancing equipment can distribute traffic by multiple firewalls (cluster).
- When the load balancer routes the traffic from the same flow ALWAYS to the same firewall (depends on the LB algorithm):
  - Firewalls do not have to share connections states!
  - Decrease processing and memory requirements of each firewall.
  - Allow for a scalable growth of traffic.
  - Makes the network less vulnerable to DoS attacks.
  - When its also responsible to distribute policies/rules is called an Orchestrator.

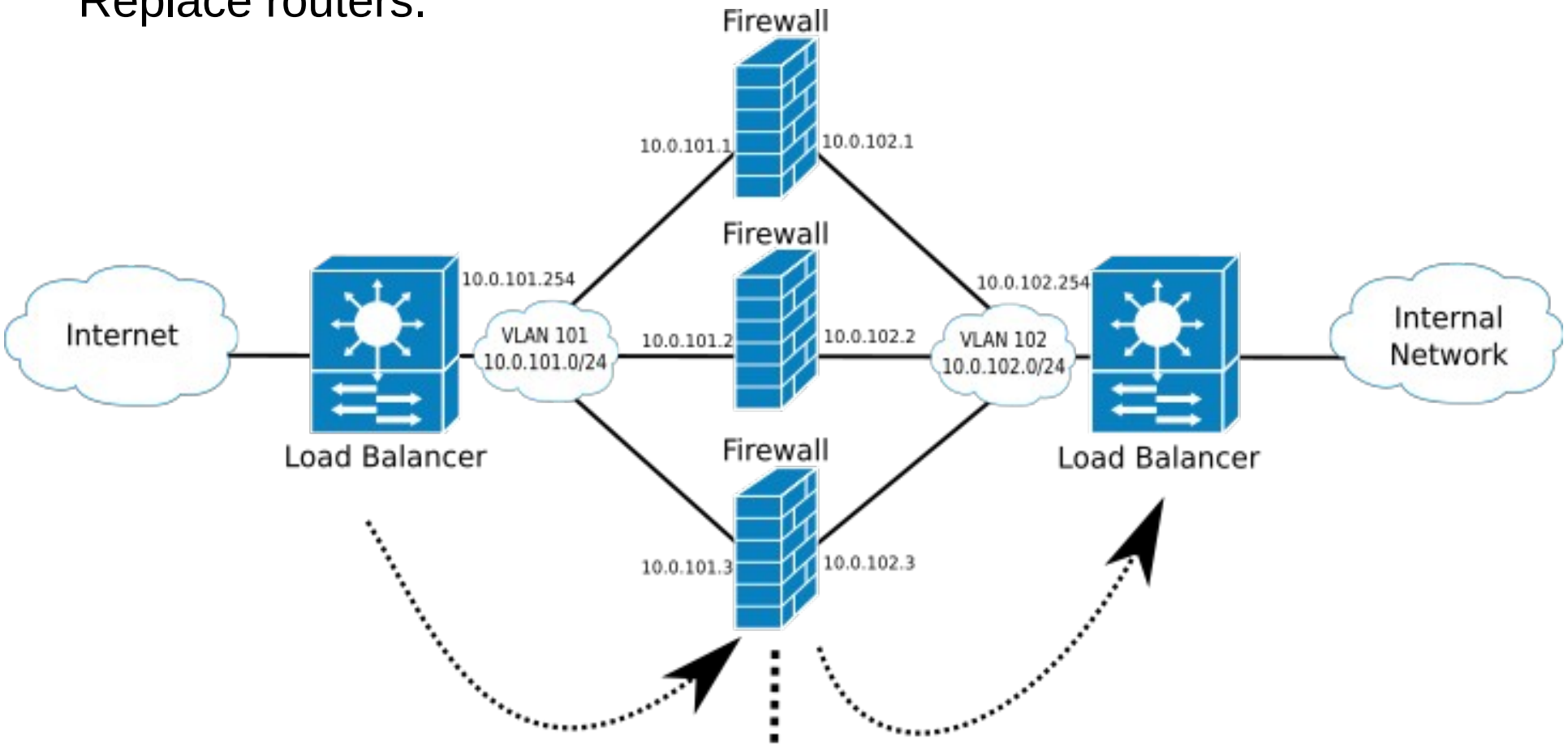


Load Balancing Algorithms

- IP Hash
  - The IP address (or a set of flow identifiers) of the client is used to determine which server/firewall receives the flow or request.
  - Does not require state synchronization (FW or LB). Hash function output determines target.
- Round Robin or Random
  - Requests are distributed across the group of devices sequentially.
  - If firewalls do not share state, load-balancers must “memorize” the interface by witch they received the traffic from firewalls, and use the same interface to route the response traffic.
- Least Connections
  - A new request is sent to the server/firewall with the fewest current connections.
  - The relative computing capacity of each server/firewall is factored into determining which one has the least connections.
  - If firewalls do not share state, load-balancers must “memorize” the interface by witch they received the traffic from firewalls, and use the same interface to route the response traffic.
- Centralized/“Smart”
  - Based on an external source of information.

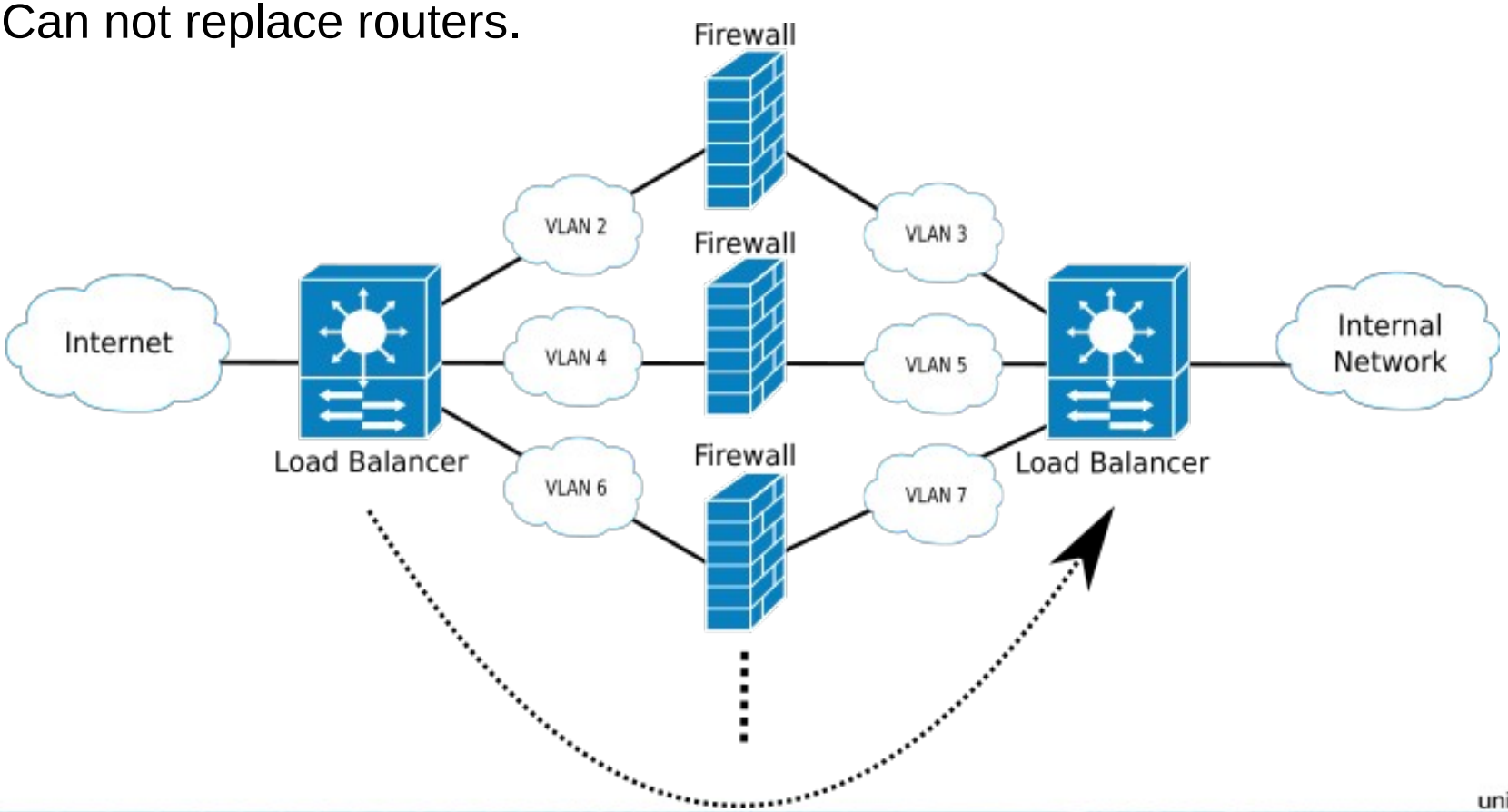
Addressed Firewalls

- Interfaces have IP addresses.
- Load balancers (or routers) route traffic as an IP next-hop.
- Can provide routing services.
  - Replace routers.



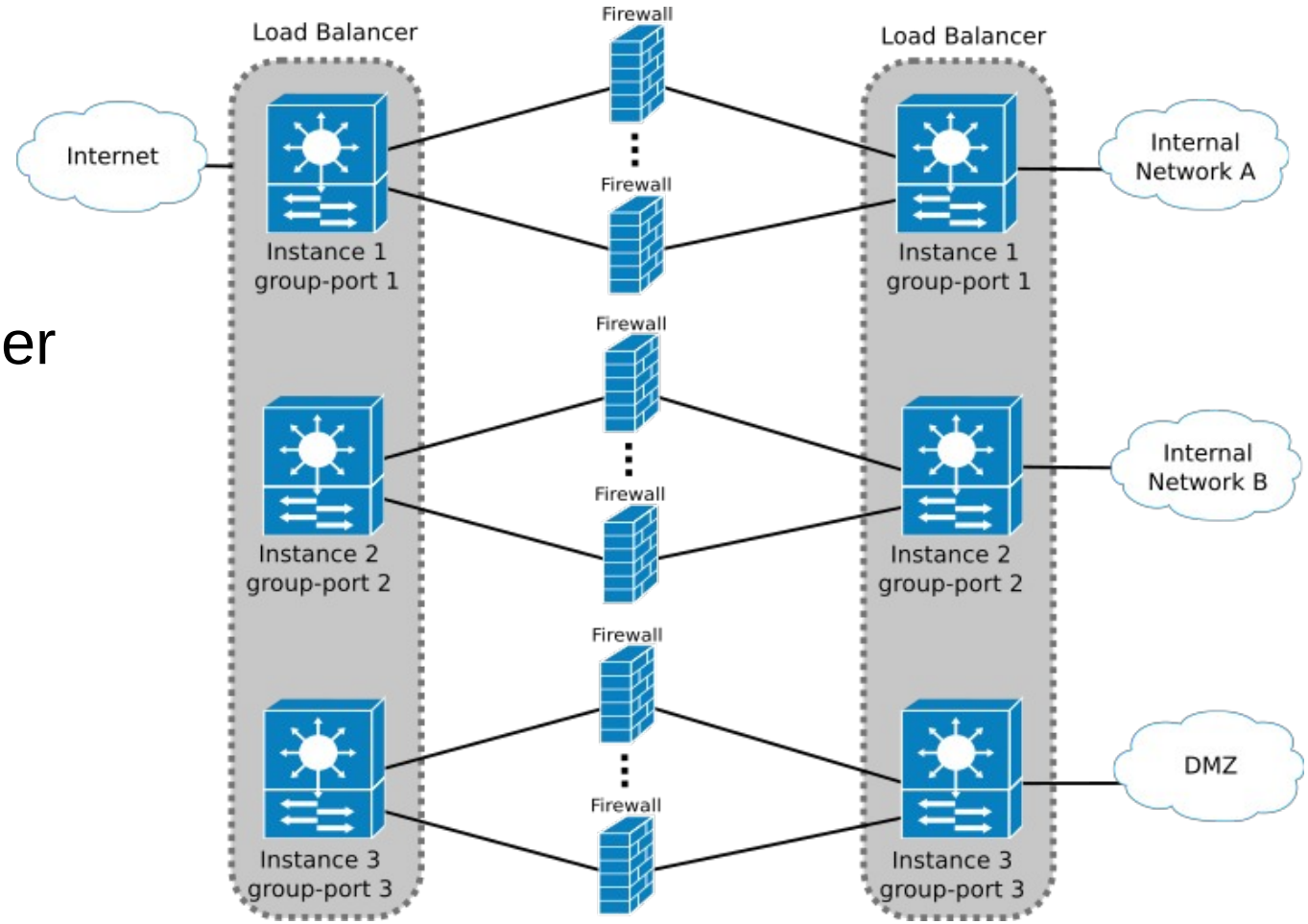
Stealth Firewalls

- Interfaces do not have IP addresses.
  - May have multiple layer rules.
- Load balancers (or swicthes) route traffic on a per interface/VLAN basis.
- Can not provide routing or NAT/PAT services.
  - Can not replace routers.



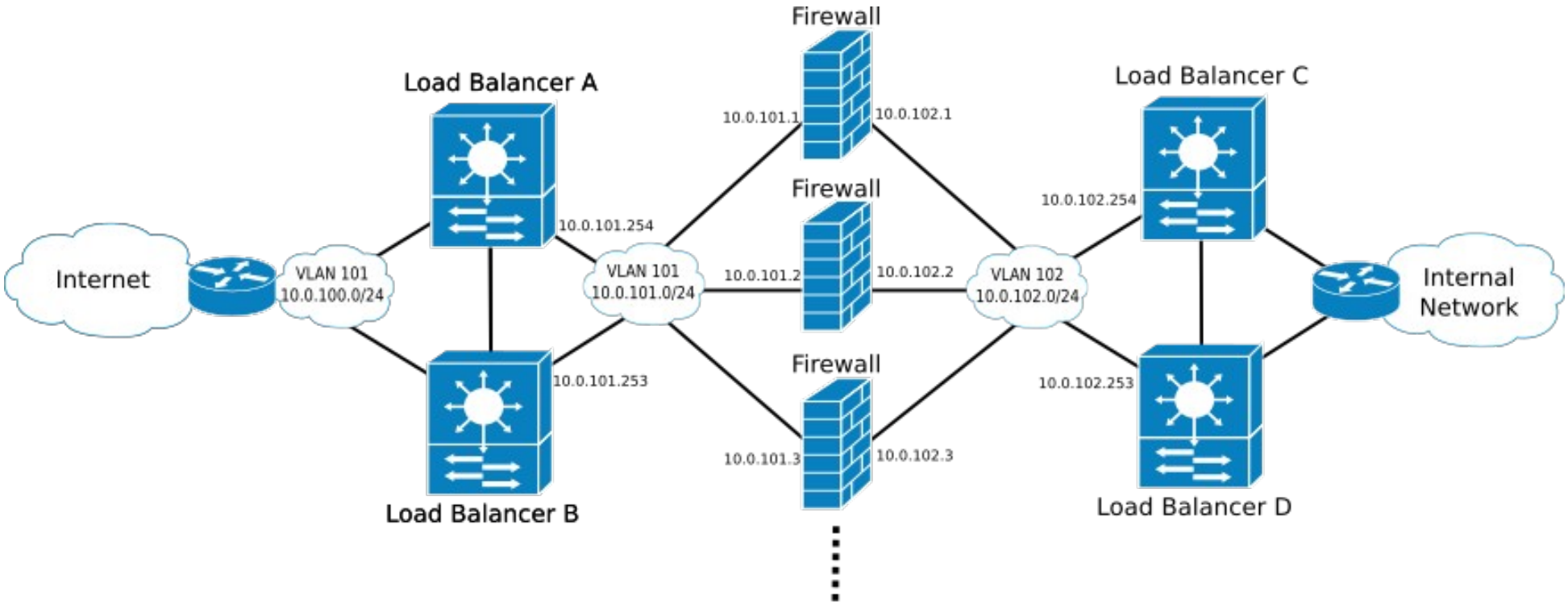
Load-Balancers Instances

- Load balancers may have (theoretical) isolated instances to handle different zones/groups.
  - With a set of firewalls per zone/group.
- Physical or virtual partitions.
- Some vendor call it group-ports.



Redundant Load Balancers

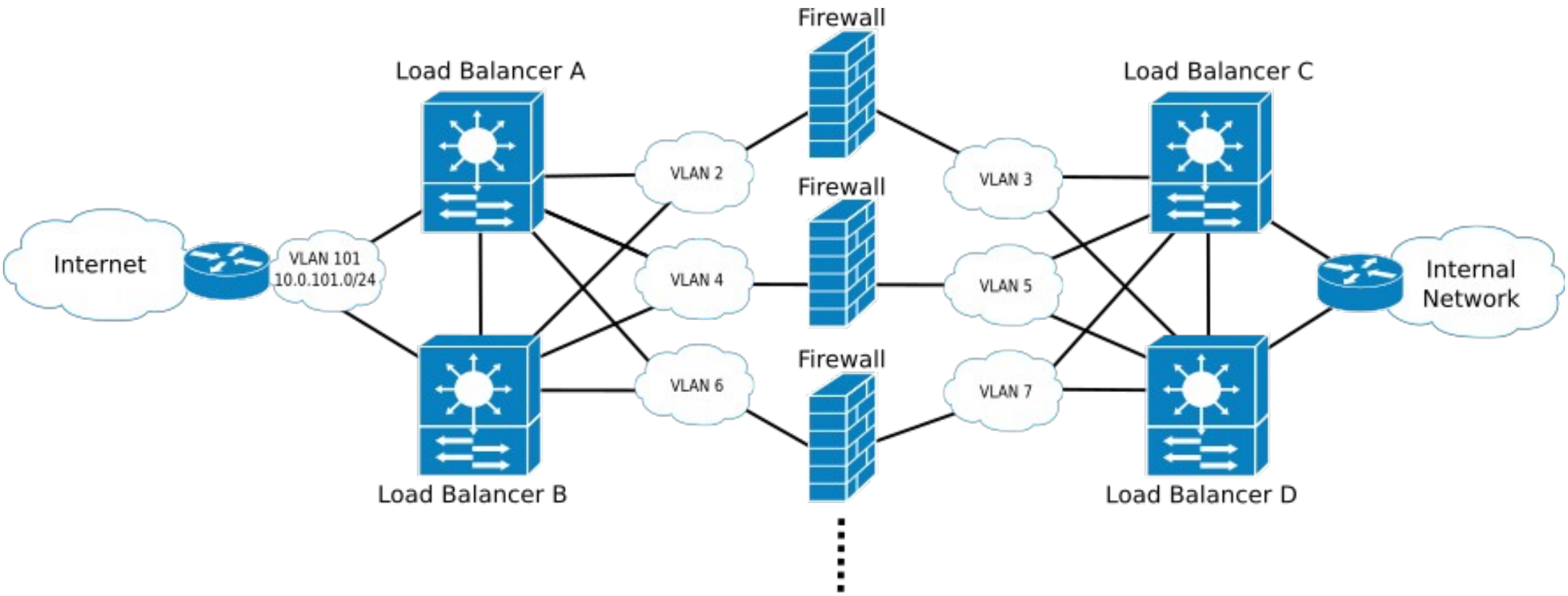
Addressed Firewalls



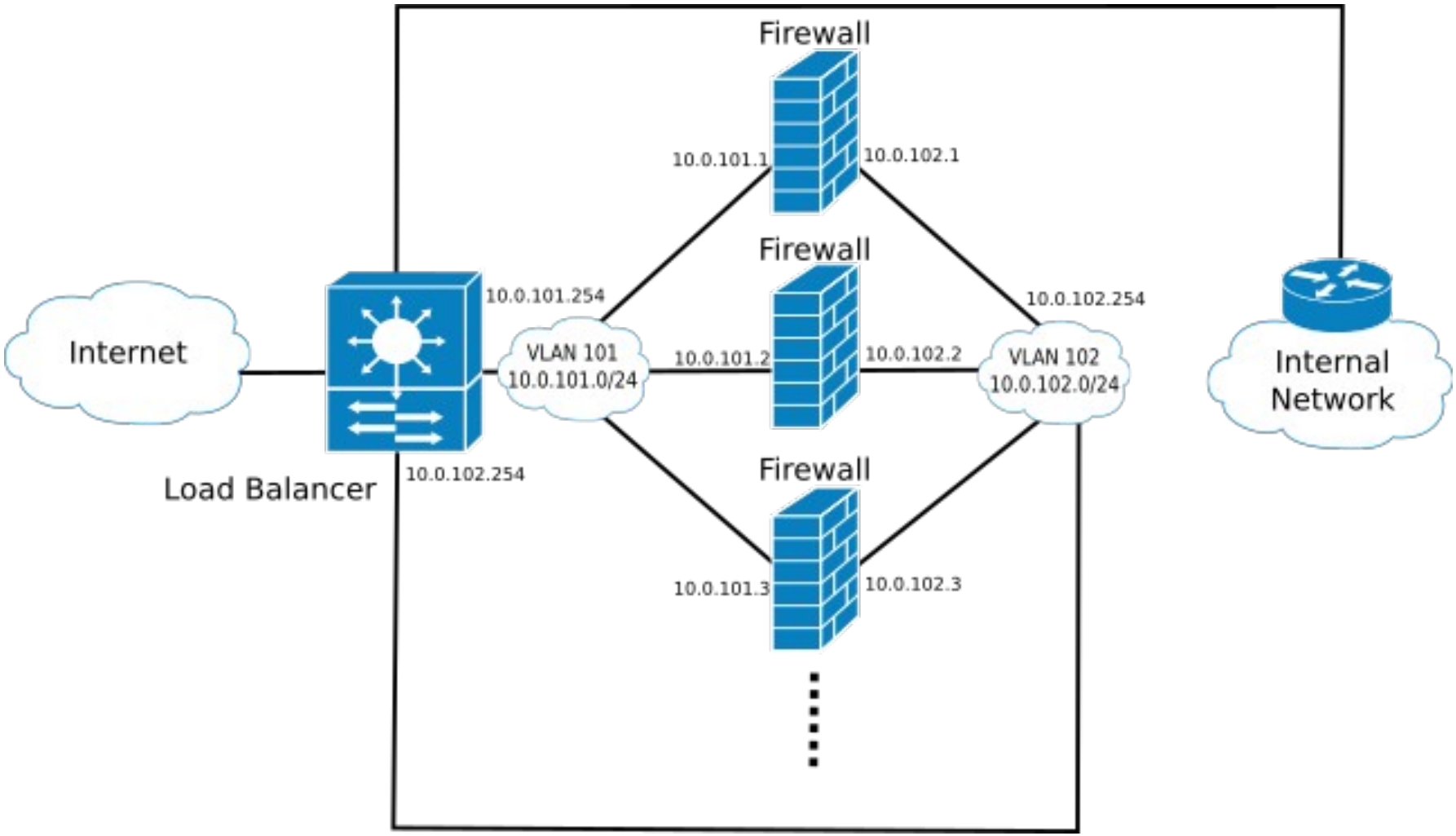
- To avoid FW state synchronizaion Load-Balancers should Sent packets of the same flow always to same firewall.
  - Must lower FW memory overload chance.
- Load-Balancers using IP Hash LB algorithms do nor require routing history synchronization (between LB).
  - Using other LB algorithms, they must share routing history.

Redundant Load Balancers

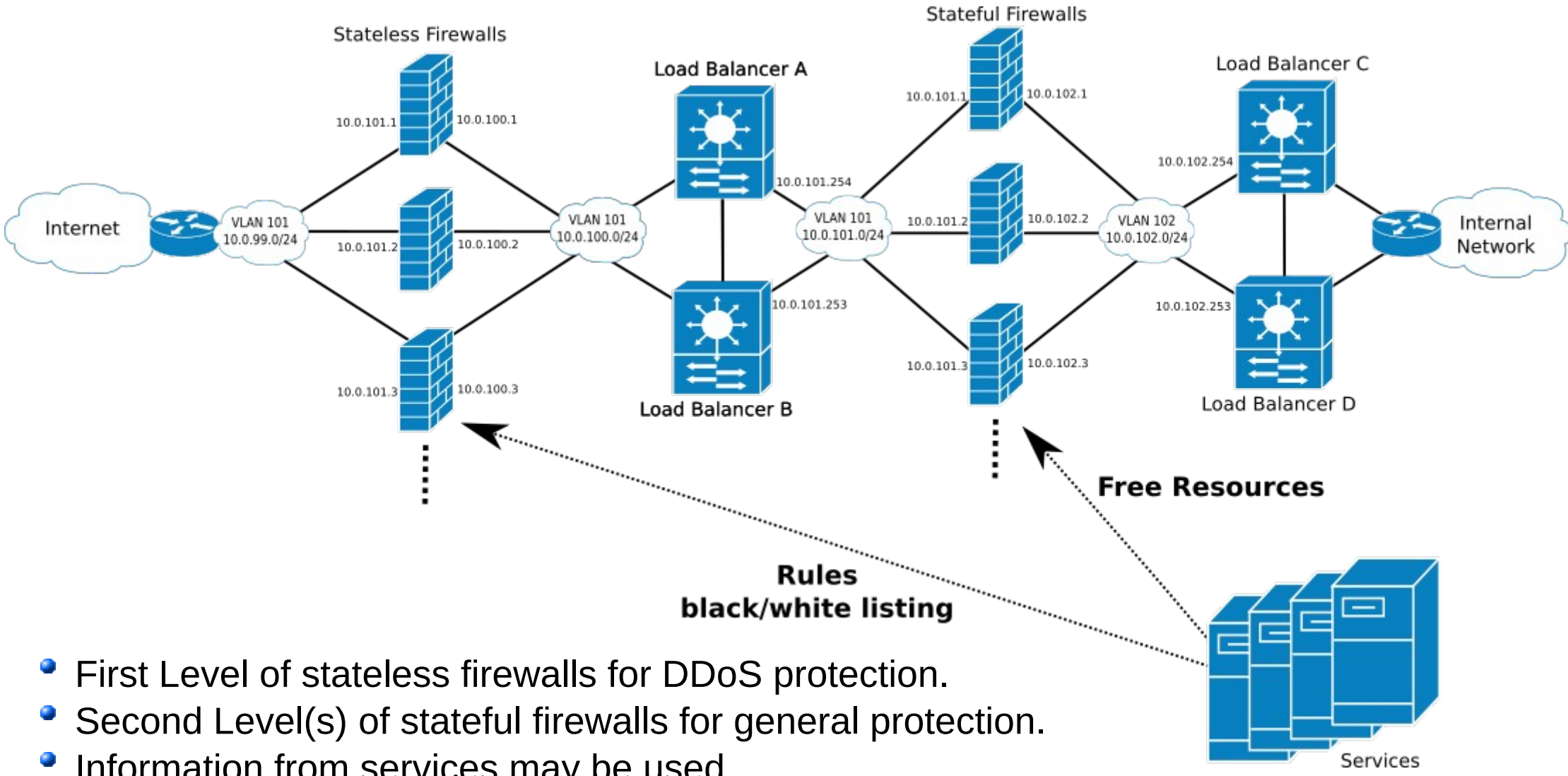
Stealth Firewalls



Single Load Balancer



Multi-Levels of Defense



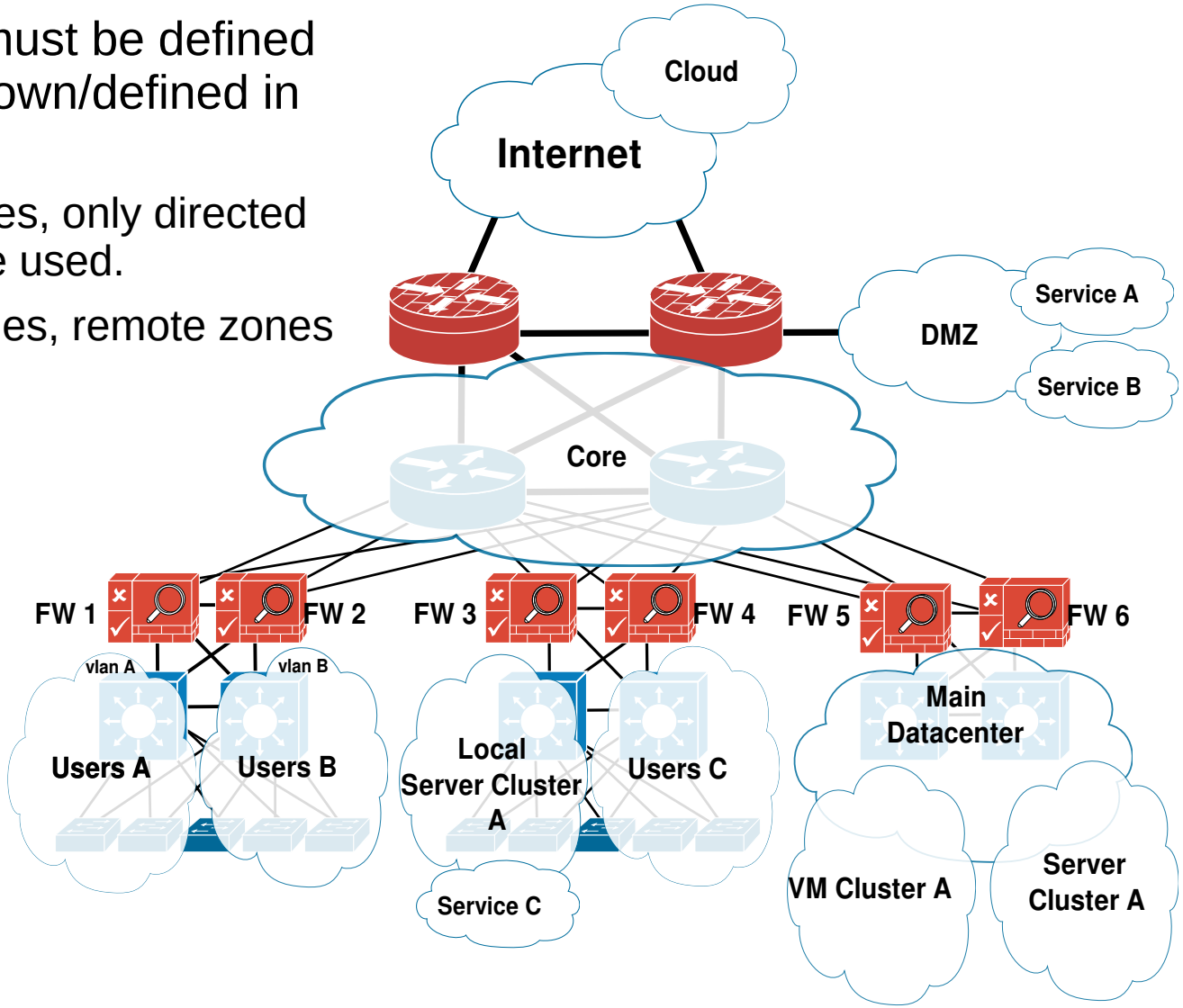
- First Level of stateless firewalls for DDoS protection.
- Second Level(s) of stateful firewalls for general protection.
- Information from services may be used
  - To free resources in the stateful firewalls.
  - To configure black/white lists rules at the stateless firewalls.

Rules (1)

- A Firewall rule (or set of rules, aka as chains) are assigned to the input (or output) of a network interface (or set/group/zone of interfaces).
  - Will be evaluated in respect to all traffic ingressing (or egressing) an interface.
- Firewall rules must specify to which traffic they should match
  - Source and destination may be IP addresses, TCP/UDP ports, set/groups of addresses/ports, etc…
  - Type may be defined in terms of protocol or protocol specifics.
  - Rules may be specified based on the state of a connection (requires a stateful firewall) upon the observation of a packet:
    - NEW - The observed packet packet is starting a new connection, or it is associated with a connection which has not generated packets in both directions.
    - ESTABLISHED - The observed packet is associated with a connection which has generated packets in both directions.
      - Usually a specif rule only allows traffic from one direction, an ESTABLISHED rule must be defined to dynamically allow the response from the other direction.
    - RELATED - The observed packet is starting a new connection, but is associated with an existing connection, such as an ICMP error (e.g., port unreachable related to an UDP connection)
- A match to a rule determines the action to execute to flow, connection or packet.
  - Some firewalls call the actions targets.
  - Possible actions are accept, drop/reject, test with another set of rules/chain, modify packet, etc...
  - The first match determines the action.
  - **The order of the rules is critical.**
  - Some firewall allow probabilistic actions based on weights.

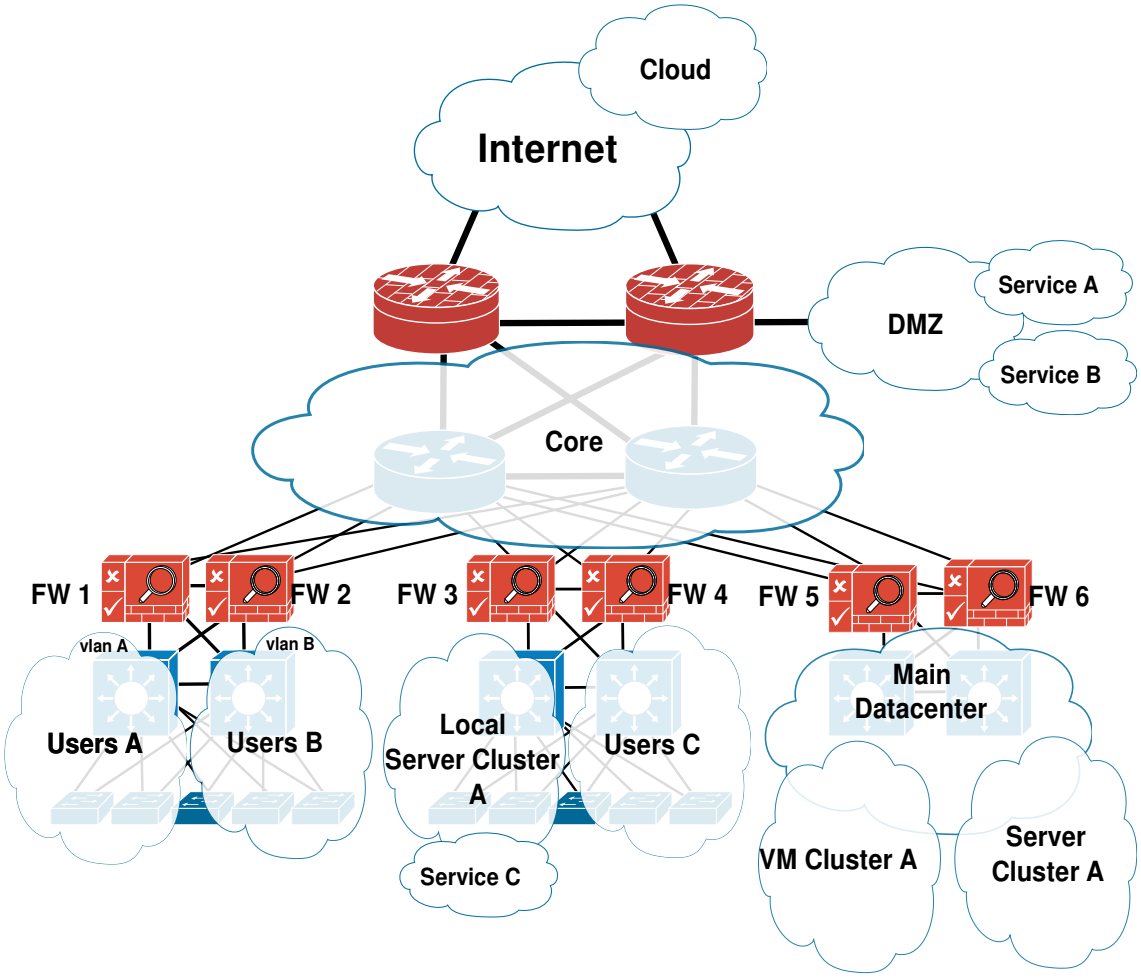
Rules (2)

- Multi zones scenarios
  - Rules in a specific FW must be defined based only on zones known/defined in that firewall.
    - For interface based zones, only directed connected zones can be used.
    - For other IDs based zones, remote zones can be used.



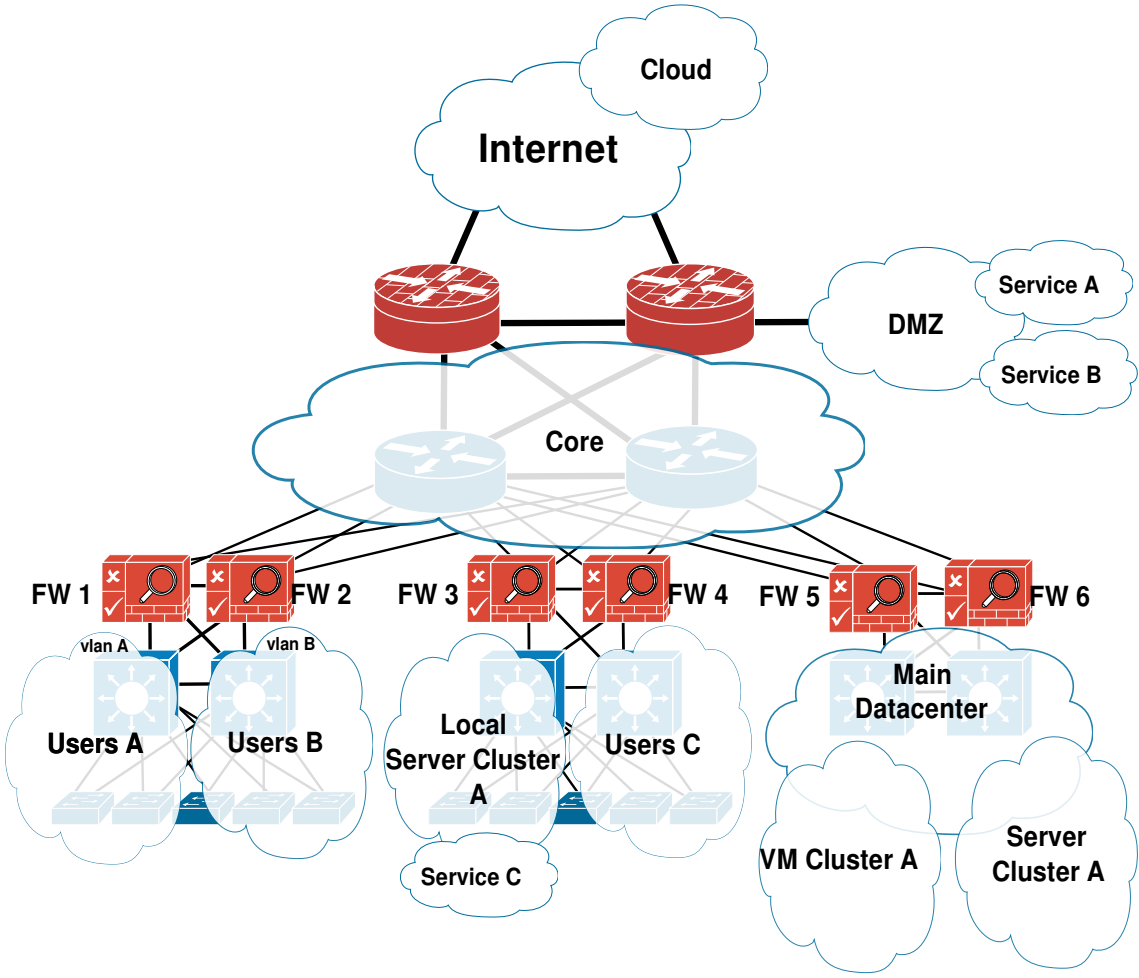
Rules (3)

- Example 1
  - Users A can access Google HTTPS services (defined by IP addresses, and TCP/UDP port 443)
    - FW1/FW2
      - Has a zone assigned to interface vlanA called **UsersA** and another zone called **Core** assigned to all core interfaces.
      - Assign a rule to the INPUT of all interfaces in zone **UsersA** and OUTPUT to any interfaces of zone **Core.**
      - Destiny of flow should be IP addresses/ports of Google Services. May specify source as IP address of specific users of vlan A.
      - Reversed rule applied from zone **Core** to zone **UsersA** allow all response traffic from established flows allowed by previous rules.
    - Main Fws
      - Has a zone assigned to all internet interfaces called **Internet** and another zone called **Core** assigned to all core interfaces.
      - Assign a rule to the INPUT of all interfaces of zone **Core** and OUTPUT to any interfaces of zone **Internet**.
      - Destiny of flow should be IP addresses/ports of Google Services. May specify source as IP address of specific users of vlan A.
      - Reversed rule applied from zone **Internet** to zone **Core** allow all response traffic from established flows allowed by previous rules.



Rules (4)

- Example 2
  - Users B may access VM Cluster A (defined by IP addresses/ports)
  - FW1/FW2
    - Has a zone assigned to interface vlanA called **UsersA** and another zone called **Core** assigned to all core interfaces.
    - Assign a rule to the INPUT of all interfaces in zone **UsersA** and OUTPUT to any interfaces of zone **Core**.
    - Destiny of flow should be IP addresses/ports VM Cluster A. May specify source as IP address of specific users of vlan A.
    - Reversed rule applied from zone **Core** to zone **UsersA** allow all response traffic from established flows allowed by previous rules.
  - FW5/FW6
    - Has a zone assigned to all interfaces/networks of VM Cluster A called **VM Cluster A** and another zone called **Core** assigned to all core interfaces.
    - Assign a rule to the INPUT of all interfaces of zone **Core** and OUTPUT to any interfaces of zone **VM Cluster A**.
    - Destiny of flow should be IP addresses/ports of IP addresses/ports VM Cluster A. May specify source as IP address of specific users of vlan A.
    - Reversed rule applied from zone **VM Cluster A** to zone **Core** allow all response traffic from established flows allowed by previous rules.

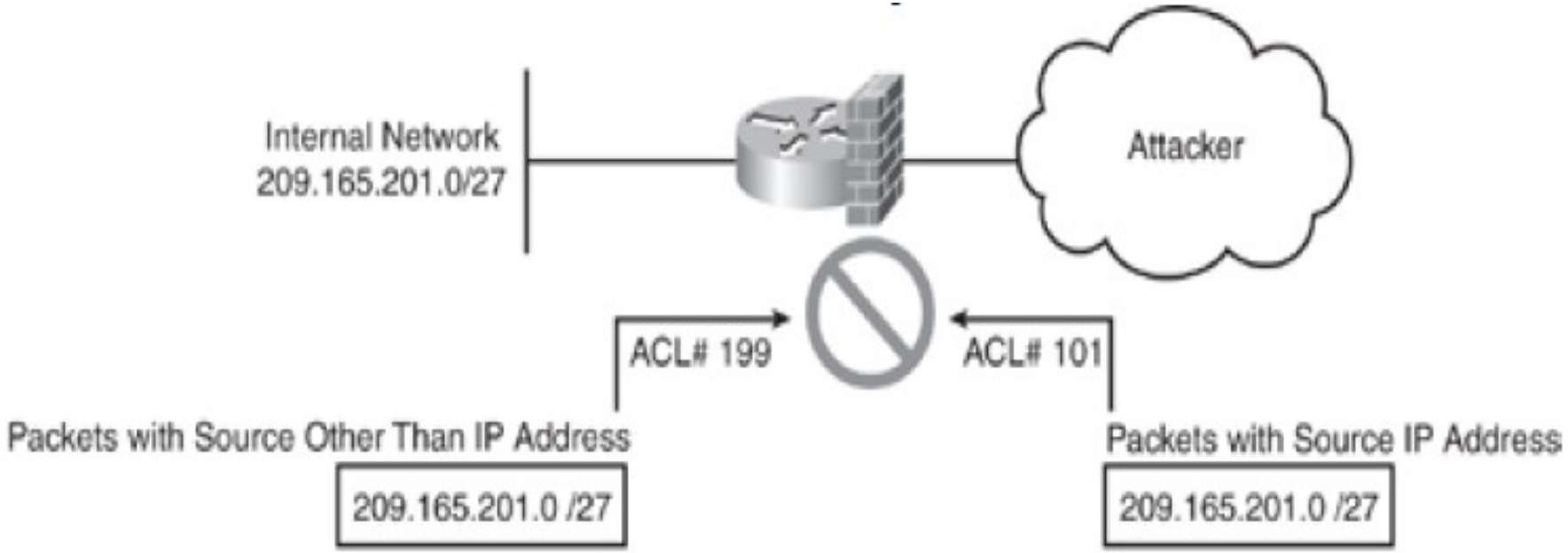


Rules (5)

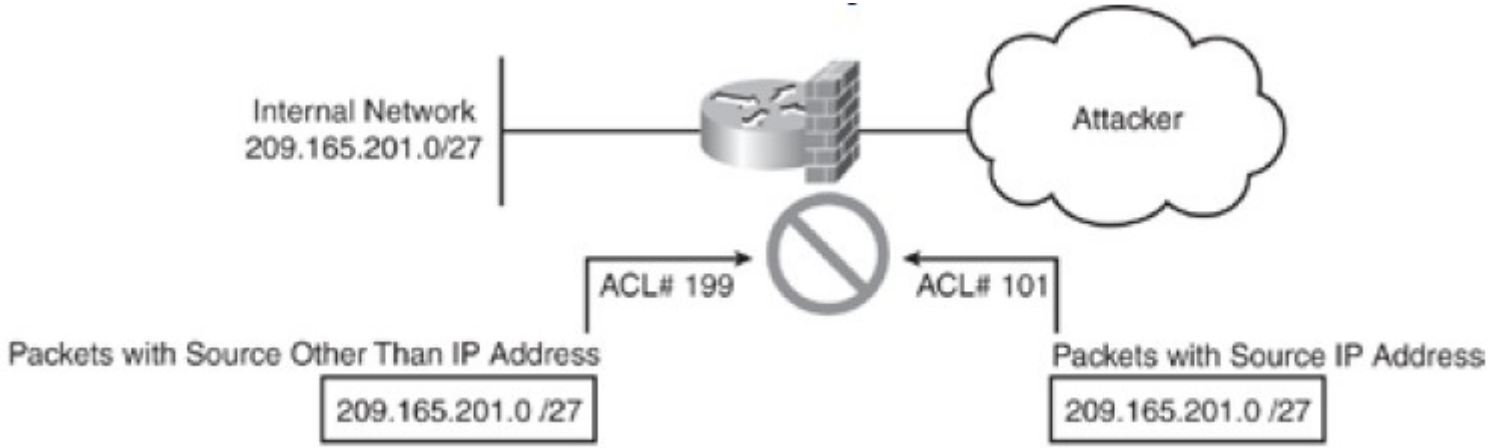
- Best Practices and Recommendations
  - Standardize your security policies.
    - Includes firewalls, network zones relations, devices and users profiles, active services, etc..
  - Define the rules the more specific as possible.
    - Avoid generic rules that may open undesired paths.
  - Blocking all traffic by default.
    - Remove “Accept All” Rules.
  - Add “Accept” exceptions.
    - Usually Clients to Service direction.
      - E.g., Internal to Internet, Internet to DMZ, etc...
      - Add reverse rule base on established /related connections.
  - Maintain documentation of firewall rules:
    - Purpose, relation to security policies, affected devices and users, deployment and expiration dates, identification of the manager.
  - Maintenance and monitoring of rules.
    - Periodically verify validity of rules within current security policies.
    - Analyze usage/match statistics of each rule.
  - Integrate flow control with existing rotting, switching and load balancing policies and services.

IP Spoofing

- IP spoofing refers to the creation of IP packets with a forged source IP address.
  - To hide the identity of the sender or impersonate another network system.
  - Spoofing IP datagrams is a well-known problem.
  - Most spoofing is done for illegitimate purposes.



Preventing IP Spoofing at Layer 3

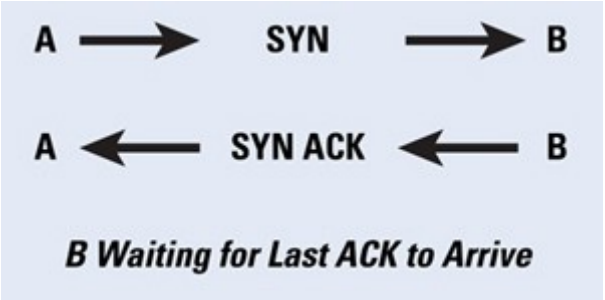


- Deny external traffic with
  - IP source equal to protected network IP ranges.
  - IP source equal to private addresses.
  - Multicast destinations.
- Reverse Path Verification
  - Deny traffic where the source IP network is not reachable using the interface where the packet arrived.

```
Interface interface-name
  ip access-group 101 in
  ip access-group 199 out
!
access-list 101 deny ip 209.165.201.0 0.0.0.31 any
access-list 101 deny icmp any any redirect
access-list 101 deny ip 224.0.0.0 31.255.255.255 any
access-list 101 deny ip 240.0.0.0 15.255.255.255 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip 10.1.1.0 0.0.0.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 permit ip any any
!
access-list 199 permit ip 209.165.201.0 0.0.0.31 any
access-list 199 deny ip any any
```

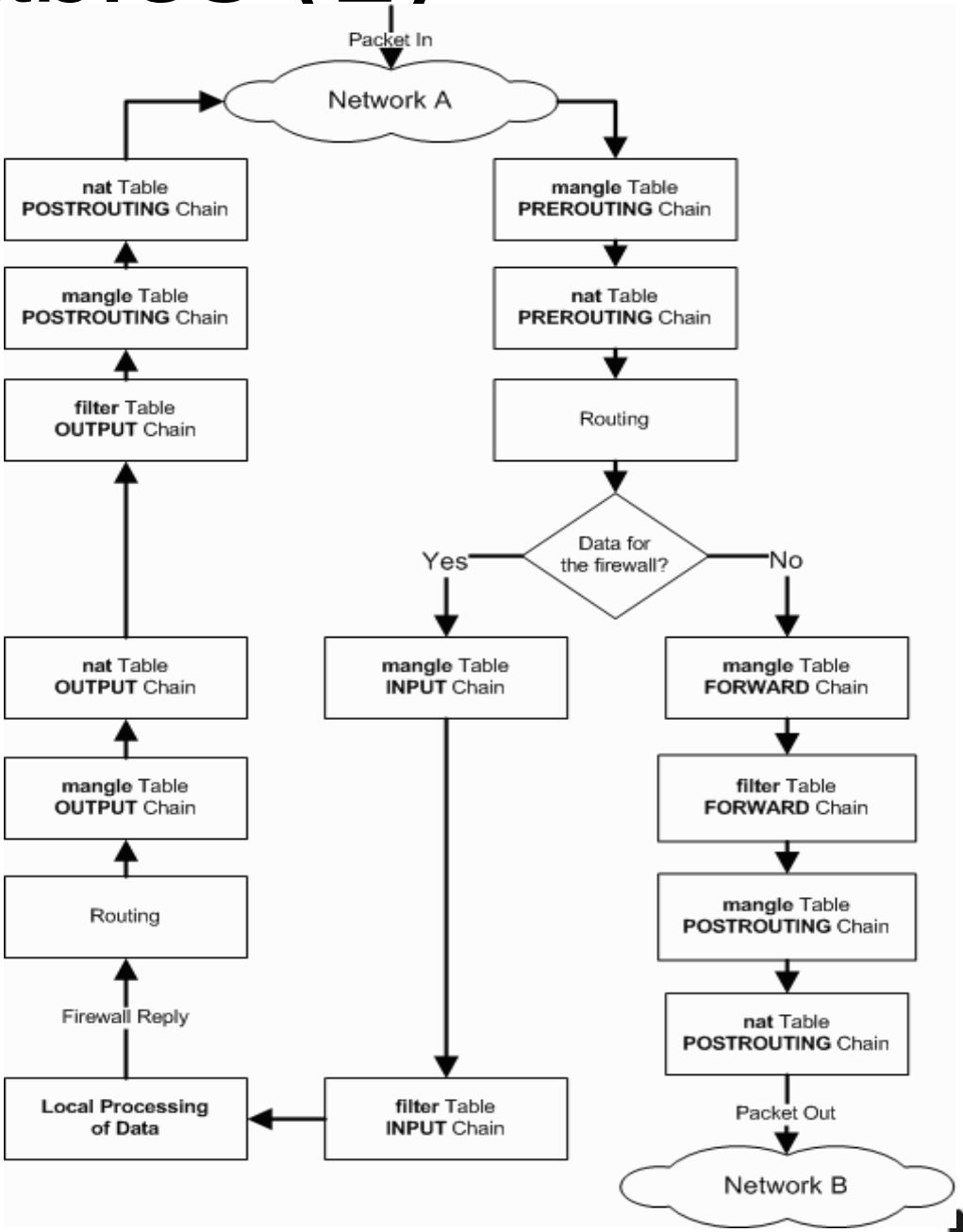
Half-Open TCP Connection Problem

- A DoS attack commonly uses half-open TCP connections.
  - Firewall keeps the state of the TCP session in memory.
  - Multiple half-open TCP connections can overrun firewalls.
    - Define timeout values for half-open TCP sessions:
      - Normal: small/medium values.
      - Under attack (based on traffic thresholds): very small values.
    - May be necessary to use external means to “clean” firewall.
      - Reseting (half-open) connections from the internal servers.



Linux iptables (1)

- Name of the user space tool by which administrators create rules for the packet filtering and NAT modules.
- Used to set up, maintain, and inspect the tables of IP packet filtering rules within the Linux kernel.
- Has 5 default chains:
  - INPUT, OUTPUT, FORWARD
  - PREROUTING
  - POSTROUTING
- Has 3 default tables,
  - Filter, nat and mangle
- Basic decisions
  - ACCEPT, DROP, QUEUE and RETURN
- Extended decisions
  - LOG, MARK, REJECT, TOS, SNAT, DNAT, MASQUERADE, REDIRECT, etc...
- Multiple state machines
  - Conntrack (connection tracker).
-



universidade de aveiro

Linux IPTables (2)

- In addition to the built-in chains, the user can create any number of user-defined chains within each table, which allows them to group rules logically.
- Each chain contains a list of rules,
  - When a packet is sent to a chain, it is compared against each rule in the chain in order.
- The rule specifies what properties the packet must have for the rule to match (such as the port number or IP address).
- If the rule does not match, then processing continues with the next rule.
- If, however, the rule does match the packet, then the rule's target instructions are followed (and further processing of the chain is usually aborted).
- Some packet properties can only be examined in certain chains,
  - For example, the outgoing network interface is not valid in the INPUT chain.
- Some targets can only be used in certain chains, and/or certain tables,
  - For example, the SNAT target can only be used in the POSTROUTING chain of the NAT table.
- The target of a rule can be the name of a user-defined chain or one of the built-in targets (ACCEPT, DROP, RETURN, DNAT, SNAT and MASQUERADE).
- You can think of a target in the same way as a subroutine.

Linux nftables

- nftables replaces iptables.
- Provides a new in-kernel packet classification framework that is based on a network-specific Virtual Machine (VM).
- Uses a new nft userspace command line tool.
  - Userspace command line tool, with no need of kernel upgrades.
    - nftables interface and iptables like interface.
- High performance through maps and concatenations.
- Smaller kernel codebase. The intelligence is placed in userspace nft command line tool.
- Unified and consistent syntax for every support protocol family.

Control By Analysis of Higher Layers

- Traffic flow control based on higher layer data/protocols only works with not ciphered traffic.
- Some firewalls provide decryption and inspection of SSL/TLS traffic.
- Traffic deciphering may be achieved using a root certificate on client machines, acting as Certificate Authority for SSL requests.
  - Firewalls must issue certificates to clients on behalf of the web servers they are connecting to.
  - Firewalls intercept SSL/TLS handshake.
  - Requires client device level changes.
- Implementing this technique is processor-intensive.
  - Results in performance degradation.
  - Can be avoided by off-loading SSL/TLS decryption to a dedicated devices.
- May break privacy/confidentiality laws and rights in some countries.

Firewall Performance Evaluation

- Basic Firewall
  - IP Throughput
    - Raw capability of the firewall to pass traffic from interface to interface
  - Latency
    - Time traffic delay in the firewall
    - Should be measured and reported when the firewall is at its operating load
- Traditional Enterprise Firewall
  - Connection Establishment Rate
    - Speed at which firewalls can set up connections
  - Concurrent Connection Capability
    - Total number of open connections through the firewall at any given moment
  - Connection Teardown Rate
    - Speed at which firewalls can teardown connections and free resources
- Next Generation Firewall
  - Application Transaction Rate
    - Capability of the firewall to secure discrete application-layer transactions contained in an open connection
    - May include application-layer gateways, intrusion prevention, or deep-inspection technology
    - Application transaction rate are highly data dependent

Extra References

- Cisco, Zero Trust Architecture (Networking Technology: Security), Pearson, August 2023, ISBN-13:978-0137899739.
- Palo Alto, High Availability Concepts.
- Palo Alto, HA Clustering Overview.
- A. Lindem, A. Dogra, RFC 9568, Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6, April 2004.

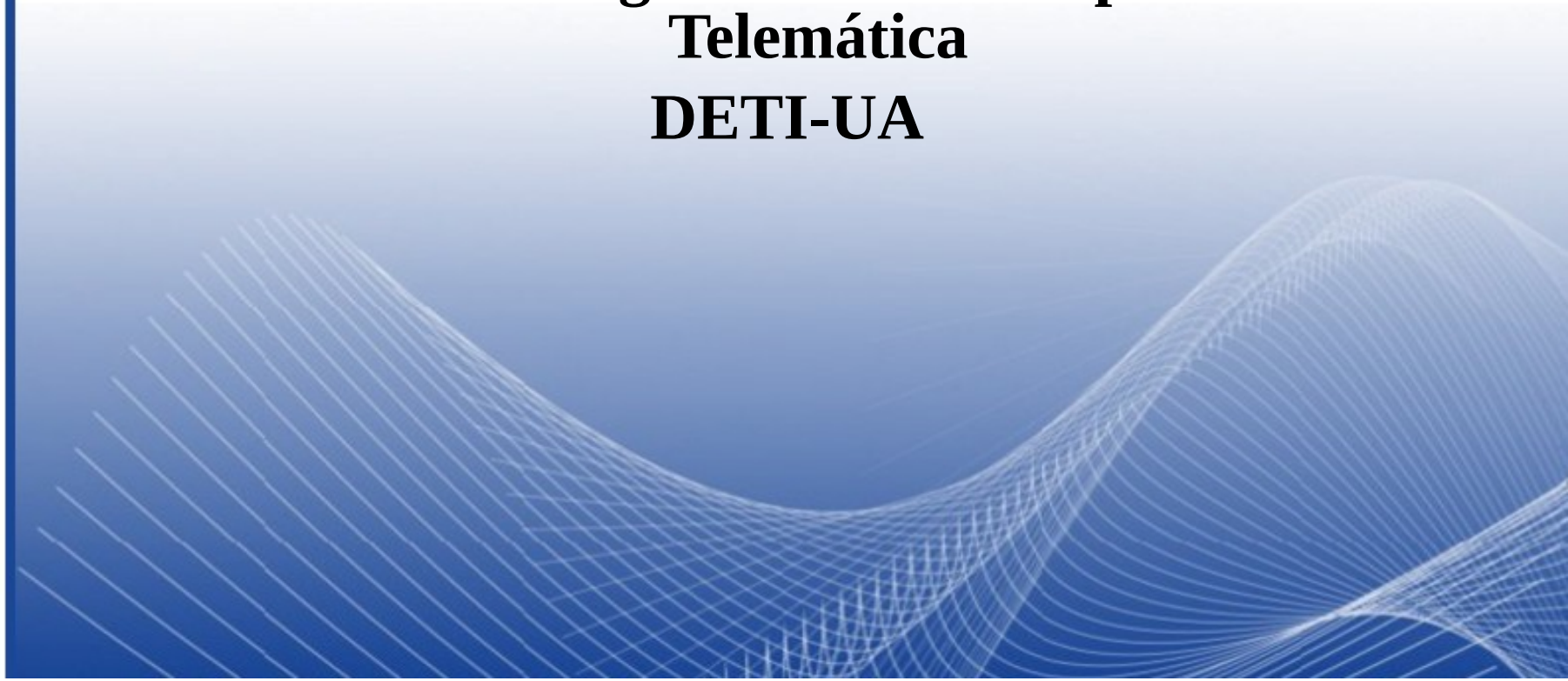
Secure Communications

Segurança em Redes de Comunicações

Mestrado em Cibersegurança

Mestrado em Engenharia de Computadores e Telemática

DETI-UA

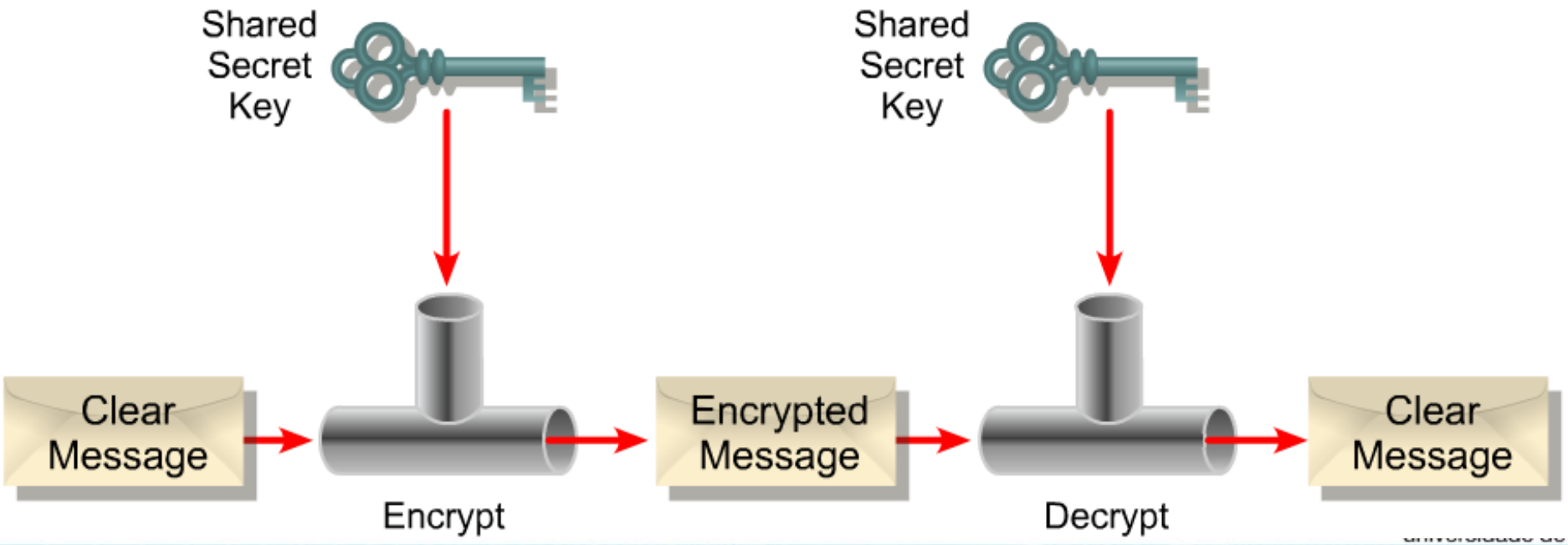


universidade de aveiro

deti.ua.pt

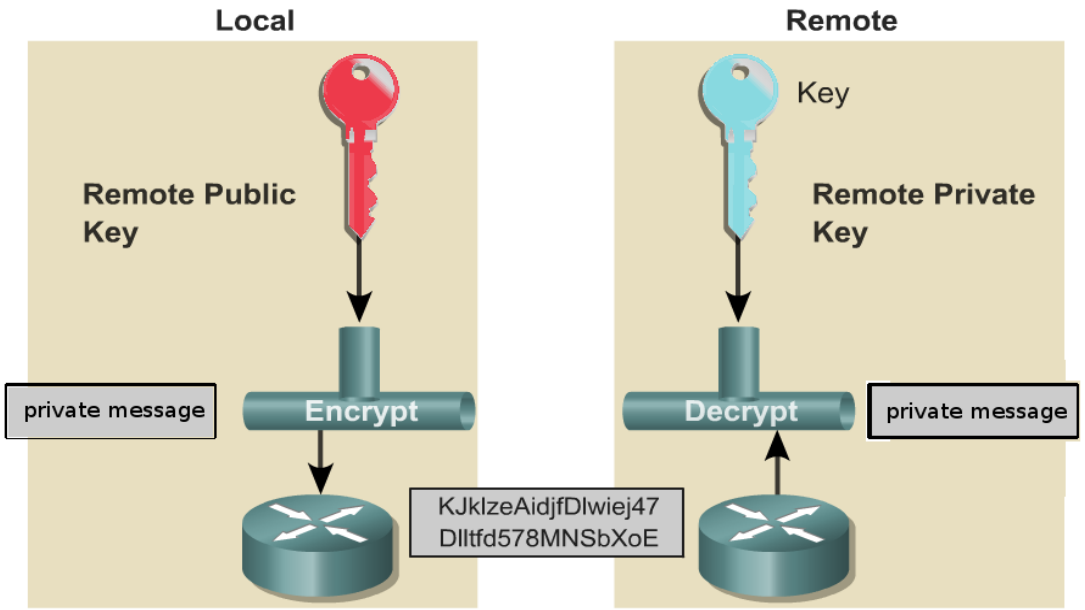
Symmetric Key Cryptography

- Two requirements for secure use of symmetric encryption:
  - Strong encryption algorithm
  - Secret key known only to sender / receiver
- Assume encryption algorithm is known
- Implies a secure channel to distribute key



Public Key Cryptography

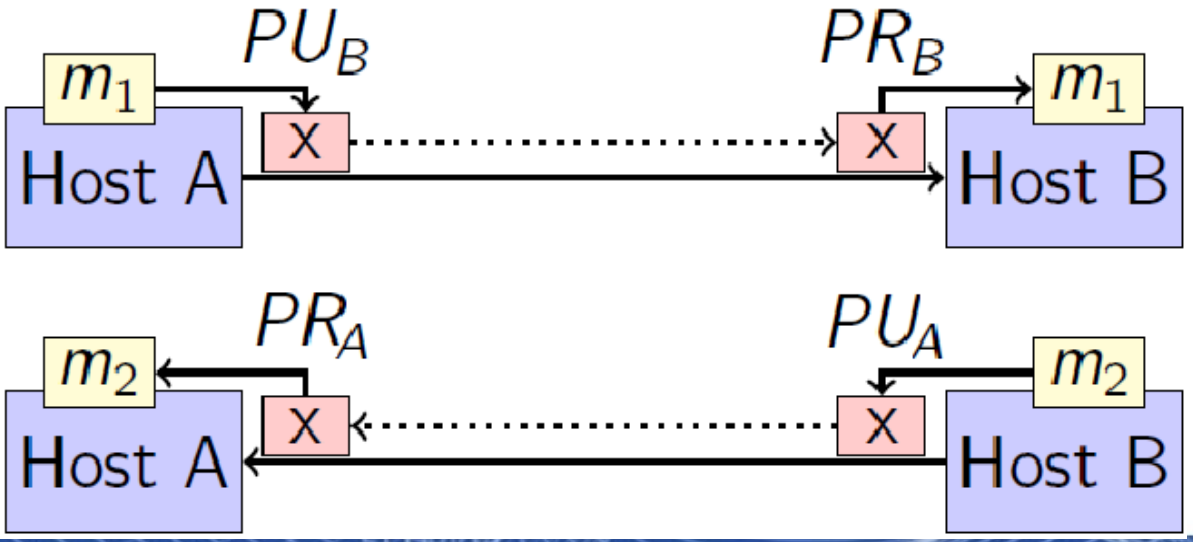
- Public Key Cryptography involves a pair of keys
- **A public key**
  - May be known by anybody, and can be used to encrypt messages, and verify signatures
- **A private key**
  - Known only to the recipient, used to decrypt messages, and sign (create) signatures



- Each public key is published, and the corresponding private key is kept secret
- Is asymmetric because those who encrypt messages or verify signatures cannot decrypt messages or create signatures

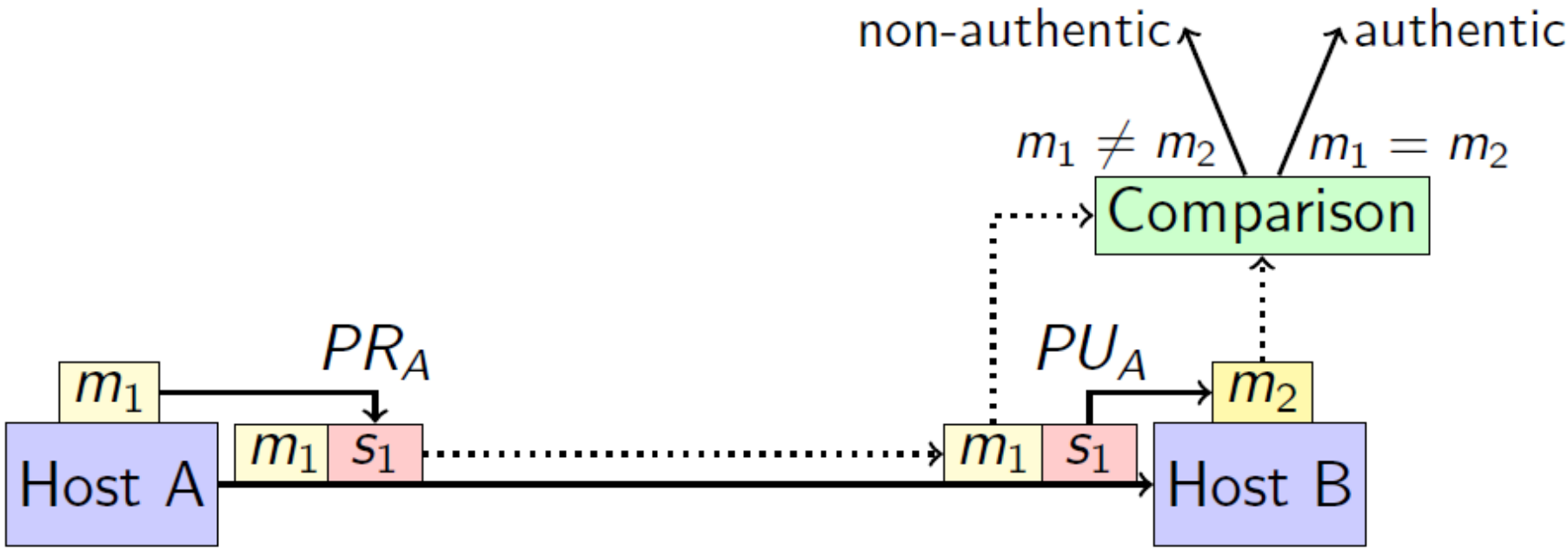
Public Key Encryption for confidentiality

- To send an encrypted message from A to B
  - Host A encrypts data with Host B public key (PUB)
  - Host B decrypts data with Host B private key (PRB)
- To send an encrypted message from B to A
  - Host B encrypts data with Host A public key (PUA)
  - Host A decrypts data with Host A private key (PRA)
- This method is computational inefficient for encrypting large amounts of data.
- Commonly used to create secure communication channels where a temporary symmetric key can be negotiated and used to encrypt large amounts of data.



Public Key
Digital signatures for authentication

- To send an authenticated message from A to B
  - Host A creates a signature by encrypting data with Host A private key (PRA)
  - Host A sends data and signature to host B
  - Host B verifies date by decrypting signature with Host A public key (PUA) and compares with received message

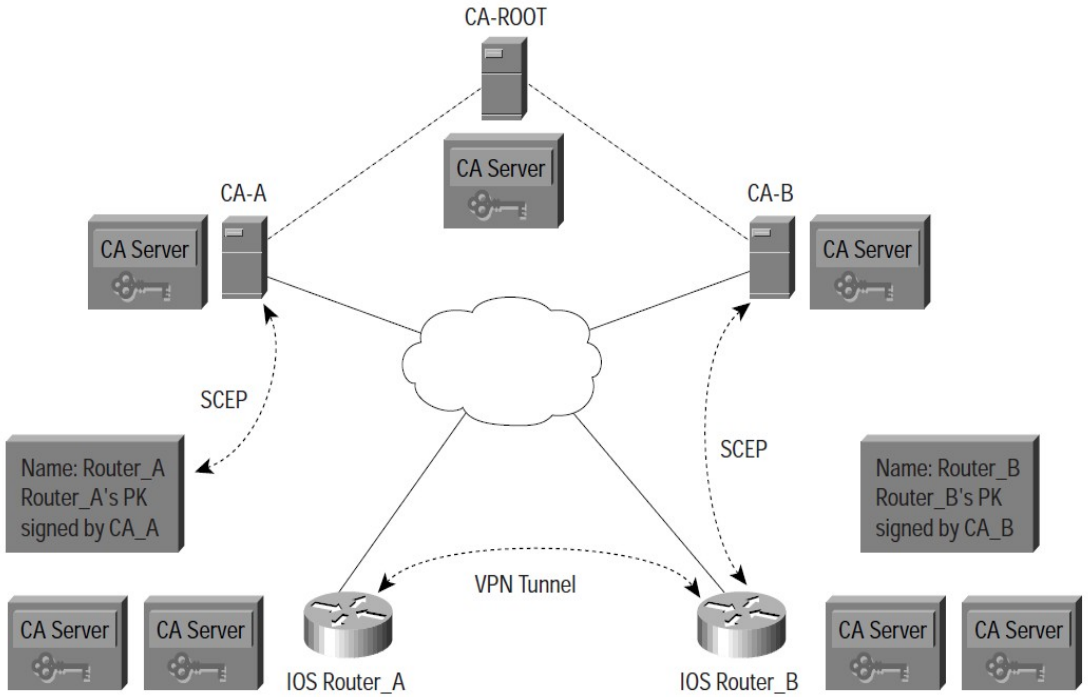


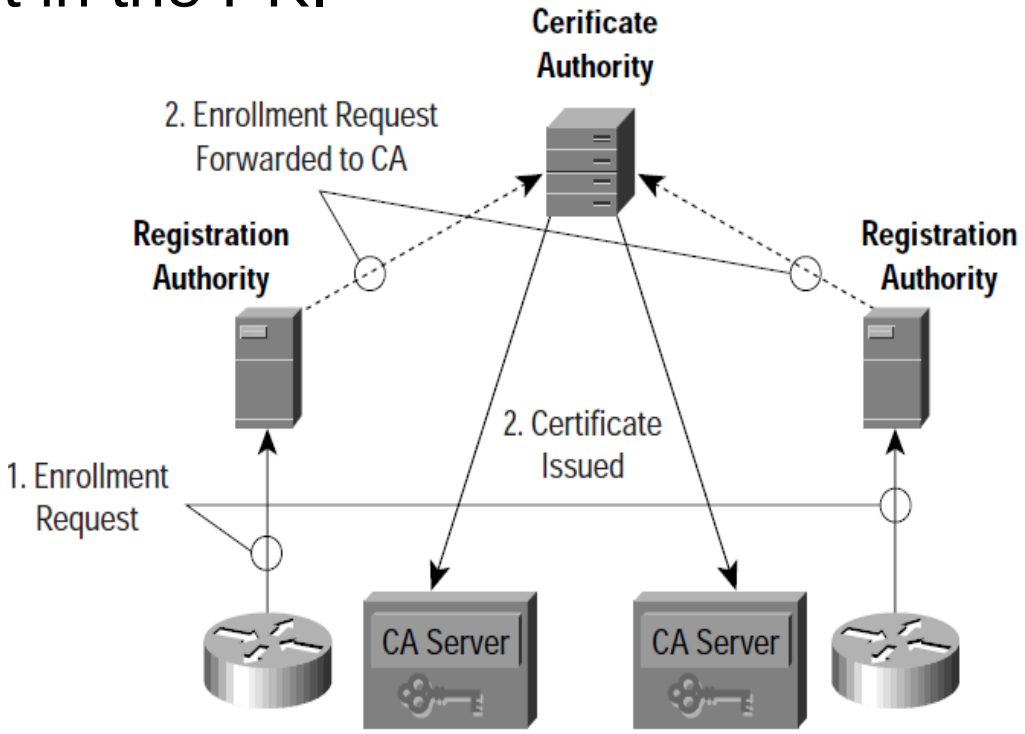
RSA (Rivest, Shamir and Adleman)

- Named after its inventors - Rivest, Shamir and Adleman
- It's a public key algorithm (encryption and decryption)
- Key length is variable
  - Common key lengths: 512, 1024 and 2048 bits
- Block size is variable but must be smaller than key length
- Ciphertext length will be the length of the key
- Slower than DES, AES and IDEA
  - Usually not used to encrypt large messages
  - Used to encrypt secret key and secret key used to encrypt messages

Public Key Infrastructure (PKI)

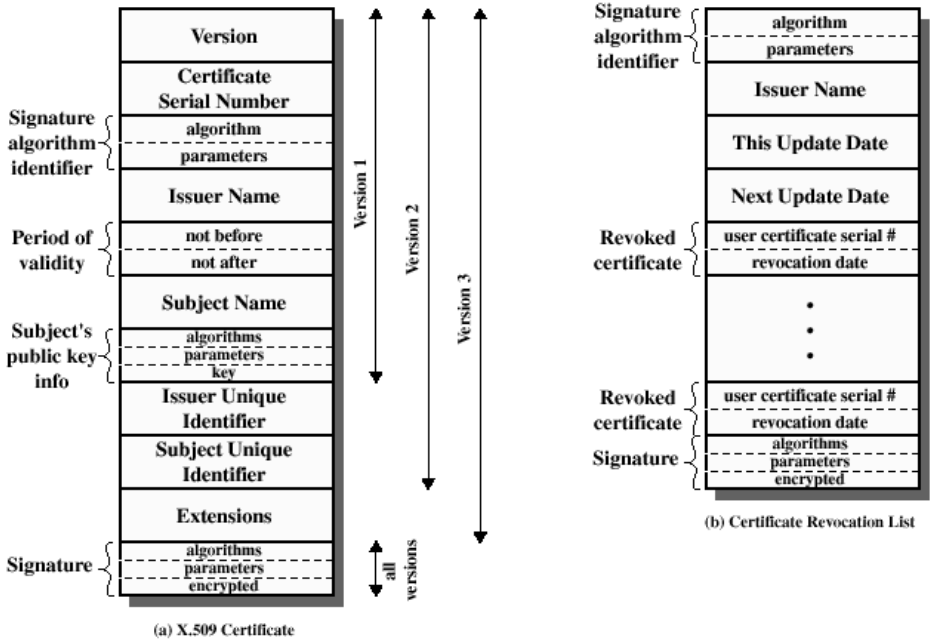
- PKIs are hierarchical in nature
- Each PKI participant holds a digital certificate that has been issued by a Certificate Authority (CA)
  - CA may be a root CA or a subordinate CA
    - Trust chain.
- PKI might use additional hosts called Registration Authorities (RA) to accept requests for enrollment in the PKI





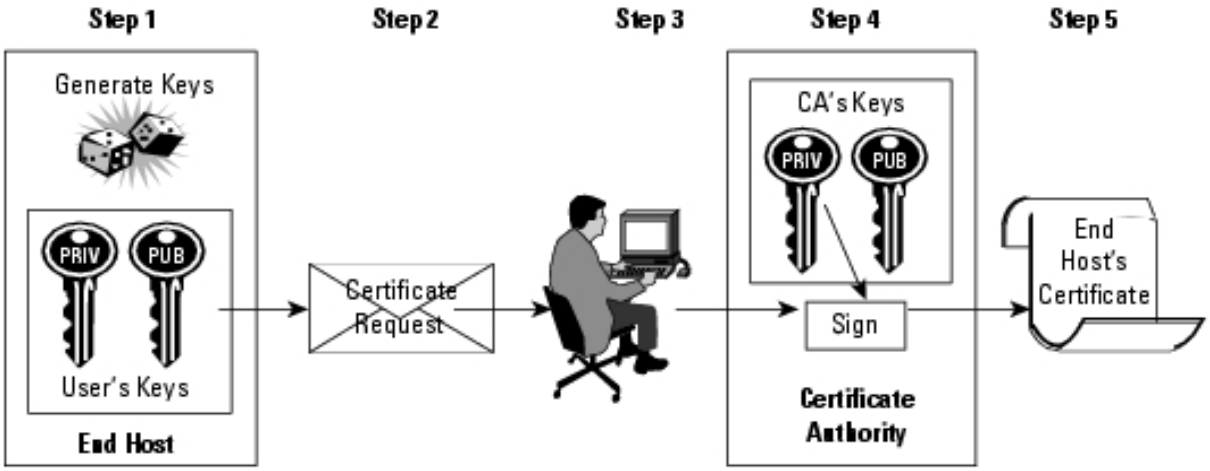
X.509 certificate contents

- Version
- Serial Number
- Signature Algorithm
- Issuer Name
- Validity Period
- Subject Name
  - Distinguished Name (DN) of the entity
  - CN=Java Duke, OU=Java Software Division, O=U.Aveiro, C=PT
- Subject Public Key Information
  - Public Key Algorithm
  - Subject Public Key
- Certificate Signature Algorithm
- Certificate Signature



Certificate Authority enrollment

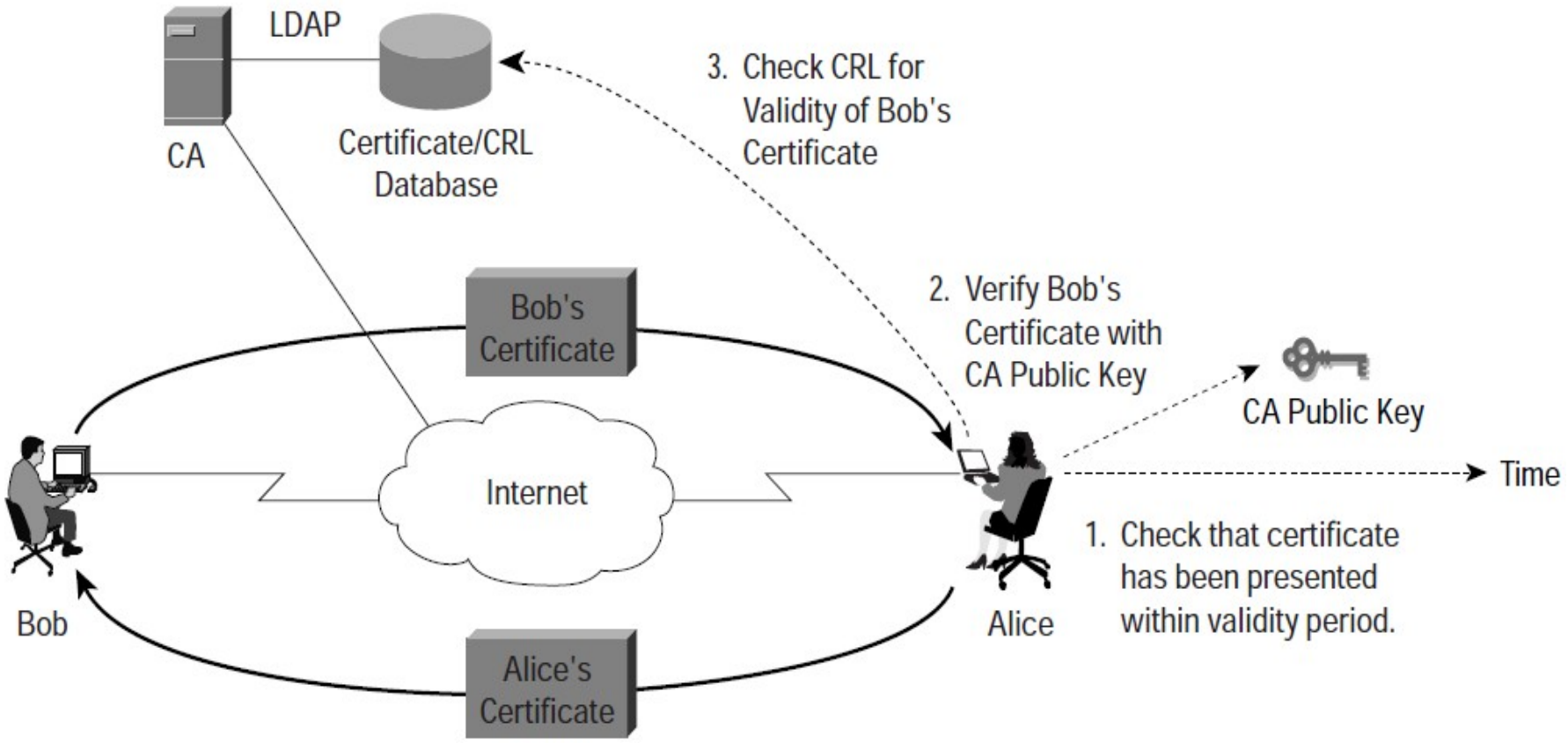
- Simple Certificate Enrollment Protocol (SCEP) is used for secure transportation of key information and certificates
- Enrolling in a Certificate Authority
  1. End host generates a private-public key pair
  2. End host generates a certificate request, which it forwards to the CA
  3. Manual, human intervention is required to approve the enrollment request,
  4. After the approval, the CA signs the certificate with its private key and returns the completed certificate to the end host
  5. End host stores certificate



Certificate Revocation Lists (CRL)

- The CRL is another crucial PKI component
- Is a list of certificates that were formerly valid within the PKI, but have been revoked for some reason
- These reasons could include any of the following:
  - Compromise of keys within certificate
  - Loss of access privileges for user/device
  - Change of PKI structure requiring certificate re-issue

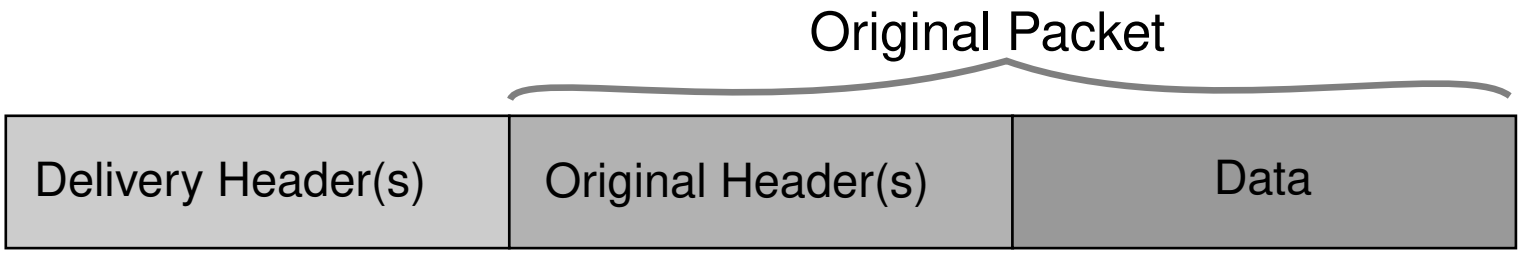
Certificate usage and validity check



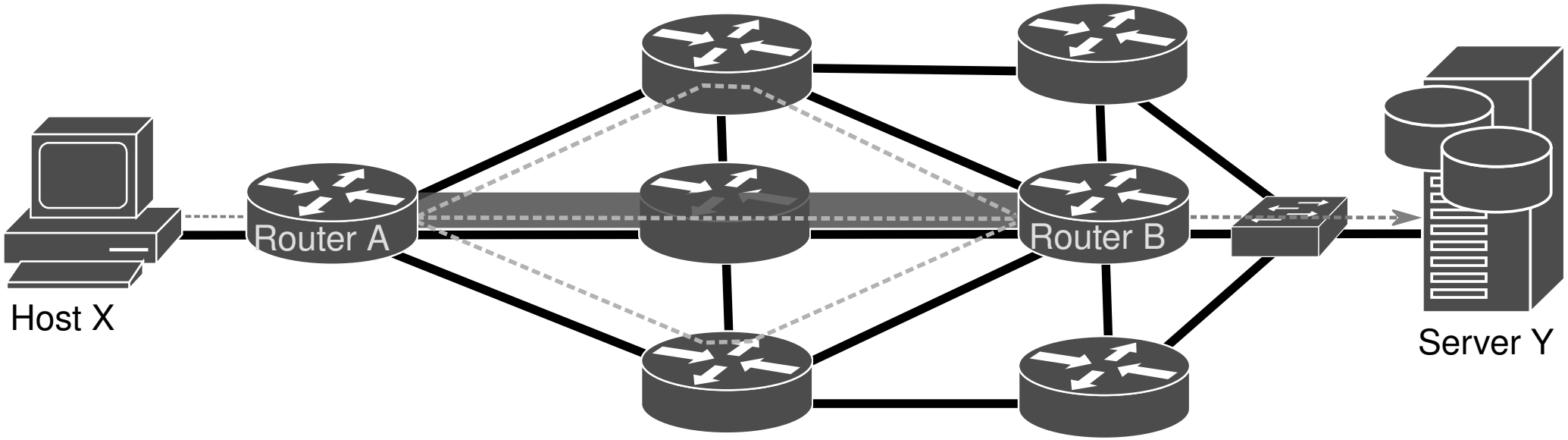
- The cert is being presented within its validity period
- The CA that signed the cert is known and trustable
- The certificate is not on a revocation list (optional in some scenarios)

Traffic Tunnel Concept

- Main purposes
  - Guarantee that a packet that reaches a network node will reach a specific secondary network node independently of the intermediary nodes routing processes,
  - Guarantee the delivery of a packet to a remote node when the intermediary nodes do not support the original packet network protocol, and,
  - Define a virtual channel that adds additional data transport features in order to provide differentiated QoS, security requirements and/or optimized routing.
- Achieved by adding, at the tunnel entry point, one or more protocol headers to the original packets to handle their delivery to the tunnel exit point.



Tunnel End-Points



Delivery protocol(s)	Original protocol(s)	Data
Source: A address Destination: B address	Source: X address Destination: Y address	

Virtual Tunnel Interface (VTI)

- Logical construction that creates a virtual network interface that can be handled as any other network interface within a network equipment.
- A tunnel does not require to have any network addresses other the ones already bound to the end-point router.
- However, most implementations impose that a network address must be bound to a tunnel interface in order to enable IP processing on the interface.
  - The tunnel interface may have a explicitly bound network address or reuse an address of another interface already configured on the router.

```
#interface Tunnel 1
 #ip address 10.1.1.1 255.255.255.252
 #ipv6 address 2001:A:A::1/64
 #ip unnumbered FastEthernet0/0
 #ipv6 unnumbered FastEthernet0/0
 #ip ospf cost 10
 #ipv6 ospf 1 area 0
 #tunnel mode ipip
 #tunnel source FastEthernet0/0
 #tunnel destination 200.2.2.2
```

VTI Requirements

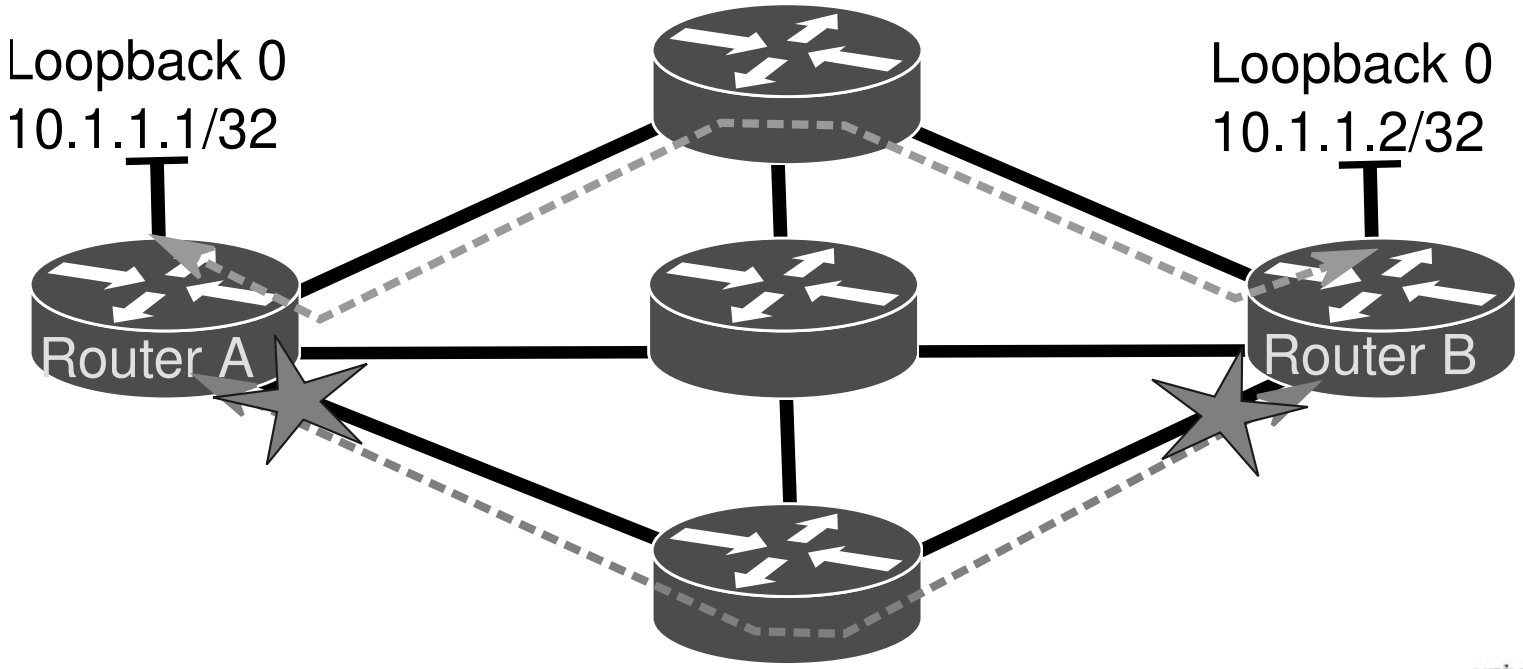
- A numeric identifier,
- A bounded IP address, this will enable IP processing,
  - Add the tunnel interface to the routing table and allow routing via the interface,

```
1  #interface Tunnel 1
2   #ip address 10.1.1.1 255.255.255.252
3   #ipv6 address 2001:A:A::1/64
4   #ip unnumbered FastEthernet0/0
5   #ipv6 unnumbered FastEthernet0/0
6   #ip ospf cost 10
7   #ipv6 ospf 1 area 0
8   #tunnel mode ipip
9   #tunnel source FastEthernet0/0
10  #tunnel destination 200.2.2.2
```

- A defined mode or type of tunnel,
  - Availability of tunnel models depends on the Router model, operating software and licenses.
- Tunnel source,
  - Defined as the name of the local interface or IPv4/IPv6 address depending on the type of the tunnel.
- Tunnel destination,
  - Defined as a domain name or IPv4/IPv6 address depending on the type of the tunnel.
  - This definition is not mandatory for all types of tunnels because in some cases the tunnel end-point is determined dynamically.
- May optionally have additional configurations for routing, security and QoS purposes.

Loopback Interfaces as End-Points

- Loopback interface is another logical construction that creates a virtual network interface completely independent from the remaining physical and logical router network interfaces.
- The main propose of a loopback interface is to provide a network address to serve as router identifier in remote network configurations and distribute algorithms.
- The main advantage of using loopback interfaces as tunnel end-points, is the creation of a tunnel not bounded to any individual network card/link that may fail.

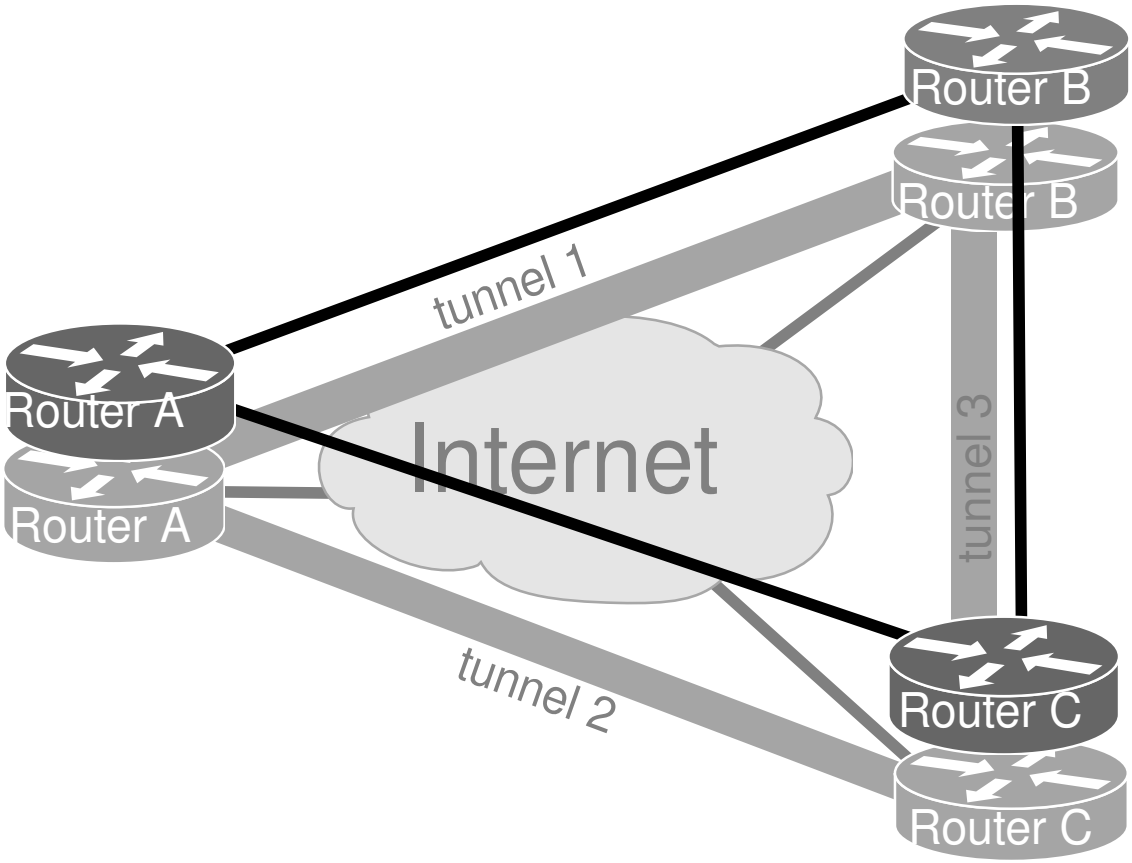


IP Tunnel Types

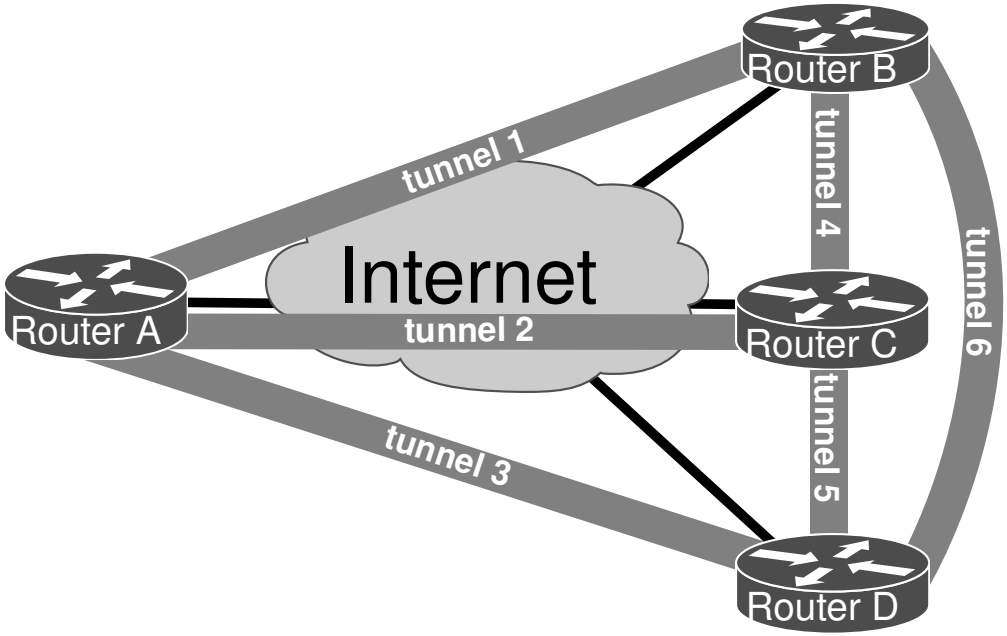
- IPv4-IPv4
  - Original IPv4 packets are delivered using IPV4 as network protocol.
- GRE IPv4
  - Original packets protocol (any network protocol) is defined by GRE header and delivered using IPv4 as network protocol.
- IPv6-IPv6
  - Original IPv6 packets are delivered using IPv6 as network protocol.
- GRE IPv6
  - Original packets protocol (any network protocol) is defined by a GRE header and delivered using IPv6 as network protocol.
- IPv6-IPv4
  - Original IPv6 packets are delivered using IPv4 as network protocol.
- IPv4-IPv6
  - Original IPv4 packets are delivered using IPv6 as network protocol.

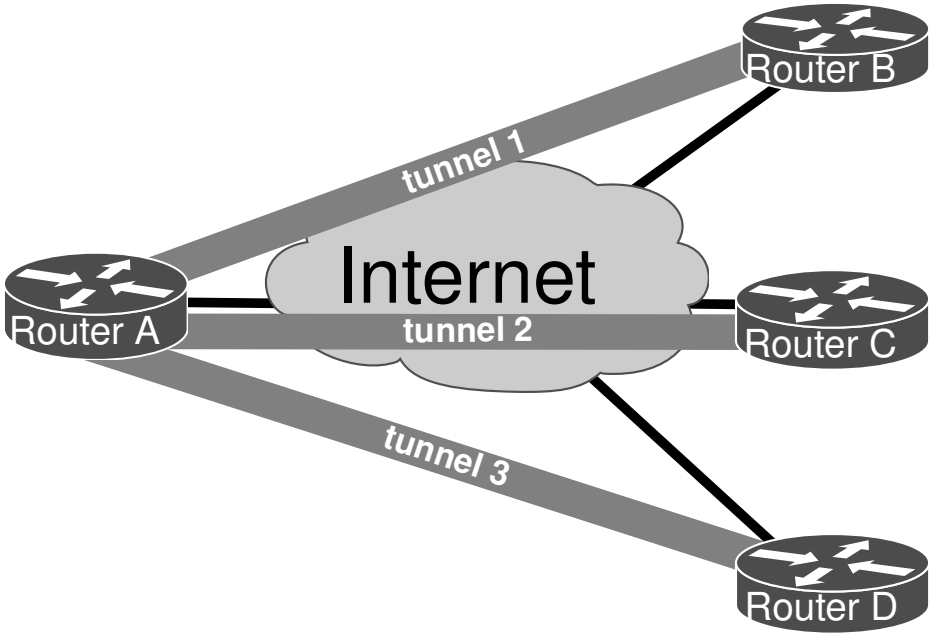
Overlay Network

- An overlay network can be defined as a virtual network defined over another network.
  - For a specific purpose like private transport/routing policies, QoS, security.
- The underlying network can be physical or also virtual.
  - May result in multiple layers of overlay networks.
- When any level of privacy protocol is present on an overlay network is designated by Virtual Private Network (VPN).



Full/Partial Overlay Mesh

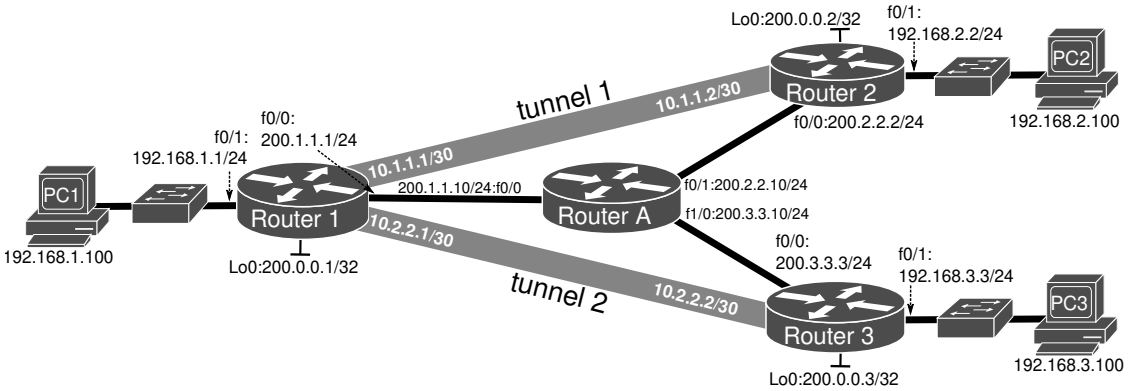




Routing Through/Between Tunnels

- Static Routes

```
#ip route 192.168.2.0 255.255.255.0 Tunnel1
#ip route 192.168.2.0 255.255.255.0 10.1.1.2
#ipv6 route 2001:A:1::/64 Tunnel1
#ipv6 route 2001:A:1::/64 2001:0:0::2
#ip route 192.168.2.100 255.255.255.255 10.1.1.2
#ipv6 route 2001:A:1::100/128 2001:0:0::2
```



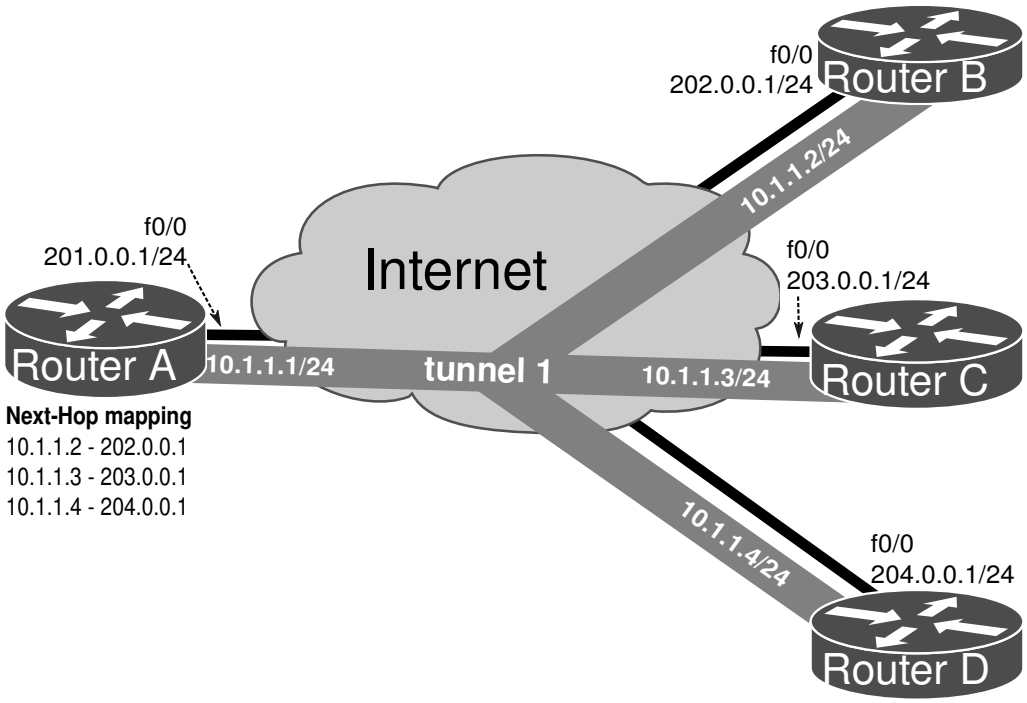
- Policy Based Routing (route-maps)

```
#access-list 100 permit ip host 192.168.1.100 192.168.2.0 255.255.255.0
#route-map routeT1
 #match ip address 100
 #set ip next-hop 10.1.1.2
#interface FastEthernet0/1
 #ip policy route-map routeT1
```

- Dynamic Routing
  - Multiple (distinct) routing processes.
    - One per overlay network, and
    - One for the underlying network.

```
#router ospf 1
 #network 200.1.1.0 0.0.0.255 area 0
 #network 200.0.0.1 0.0.0.0 area 0
!
#router ospf 2
 #network 10.0.0.0 0.255.255.255 area 0
 #network 192.168.0.0 0.0.255.255 area 1
```

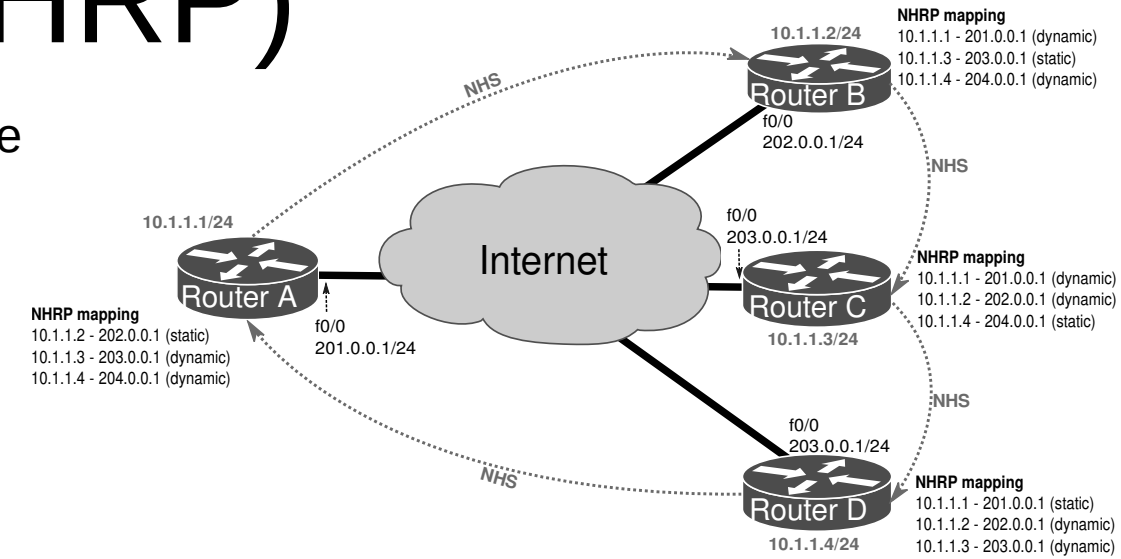
Multipoint Tunnels

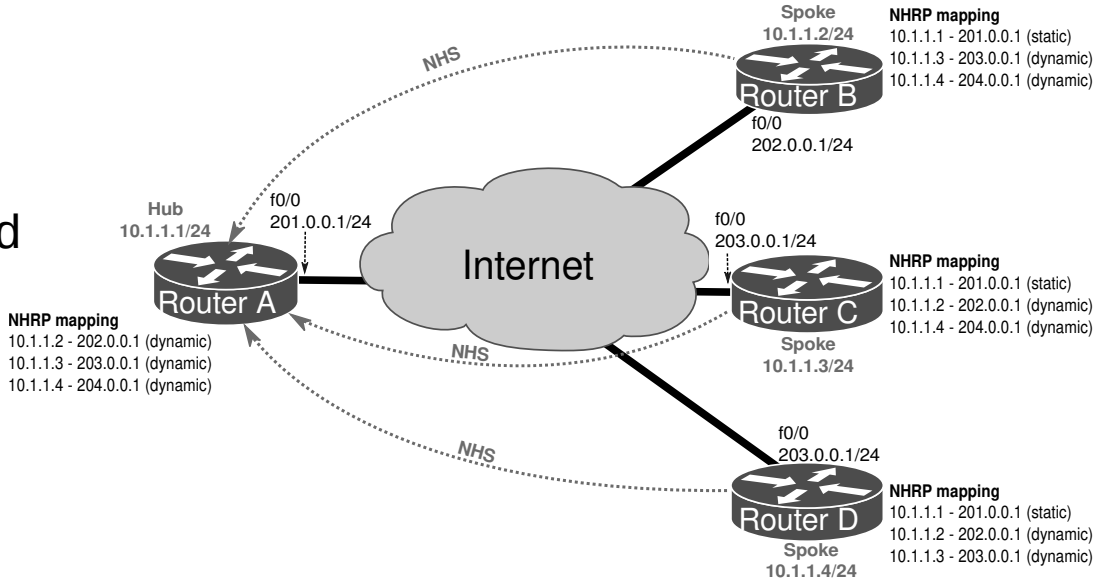


- In a scenario with many nodes to interconnect, the simpler and more efficient approach is to have a single tunnel that interconnect multiple nodes - a multipoint tunnel.
- Directly connect using a single virtual overlay IP network, defined within a multipoint tunnel.
- In a multipoint tunnel scenario, the delivery header address is determined based on the address of the next hop within the overlay network.
- Address mapping between overlay and underlying network addresses may be statically defined or dynamically obtained.

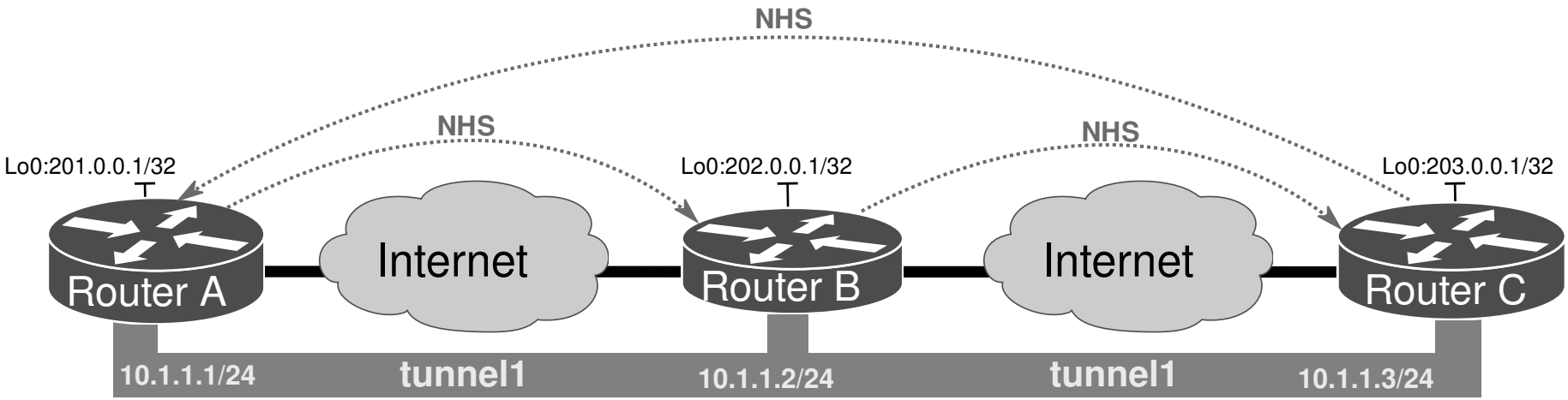
Next Hop Resolution Protocol (NHRP)

- NHRP allows to map a tunnel interface IP address (overlay network) to the respective underlying network interface IP address.
- NHRP tunnel requires that all intervening nodes should be able to find a path to any of the other nodes.
- Each node should at least know one other overlay node (and respective overlay and underlaying addresses) through which he will try to find the other nodes address mappings.
  - Next Hop Server (NHS).
- Moreover, all nodes must be configured in a way that all nodes have at least one valid path to all other nodes - forming a partial mesh.





NHRP Information Exchange



NHRP mapping
10.1.1.2 - 202.0.0.1 (static)

NHRP Register Request
10.1.1.1 - 201.0.0.1

NHRP Register Reply
10.1.1.1 - 201.0.0.1
Responder Address Extension
10.1.1.2 - 202.0.0.1

NHRP Register Request
10.1.1.2 - 202.0.0.2

NHRP mapping
10.1.1.1 - 201.0.0.1 (static)

NHRP Register Reply
10.1.1.2 - 202.0.0.1
Responder Address Extension
10.1.1.3 - 203.0.0.1

NHRP mapping
10.1.1.1 - 201.0.0.1 (static)
10.1.1.2 - 202.0.0.1 (dynamic)

NHRP Resolution Request
10.1.1.1 - 201.0.0.1
10.1.1.3 - ?

NHRP Resolution Reply
10.1.1.1 - 201.0.0.1
10.1.1.3 - 203.0.0.1
Responder Address Extension
10.1.1.2 - 202.0.0.1

NHRP mapping
10.1.1.2 - 202.0.0.1 (static)
10.1.1.3 - 203.0.0.1 (dynamic)

NHRP Resolution Request
10.1.1.2 - 202.0.0.1
10.1.1.3 - ?

NHRP Resolution Reply
10.1.1.2 - 202.0.0.1
10.1.1.3 - 203.0.0.1
Responder Address Extension
10.1.1.3 - 203.0.0.1

If "10.1.1.3 - 203.0.0.1" entry not on RouterB NHRP mapping

Hub-Spoke vs. Spoke-Spoke

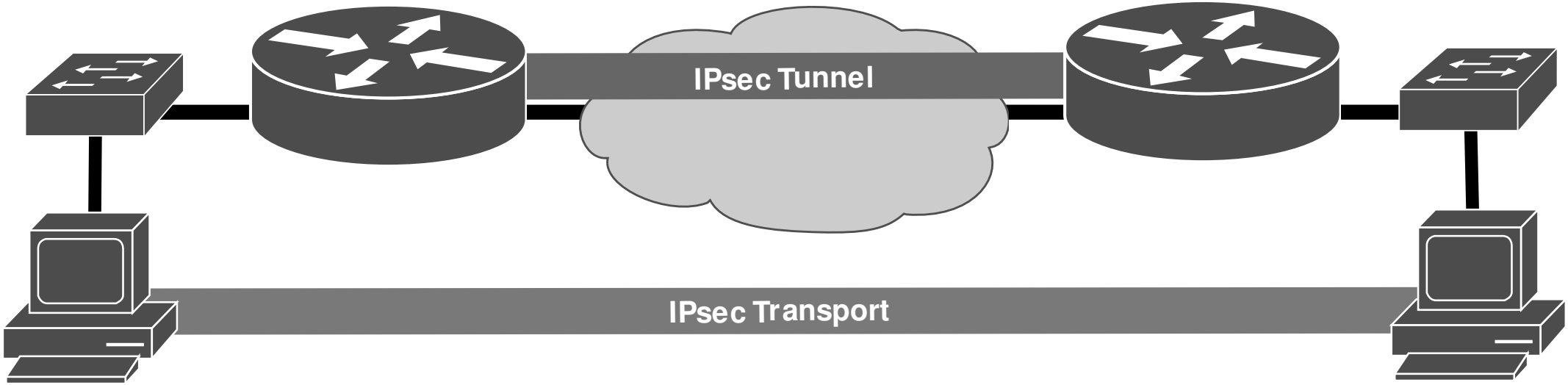
- Hub-Spoke
  - Each remote site is connected with a point-to-point GRE tunnel to a pre-defined central node (Hub).
  - Hub accepts new tunnel connections from Spokes (branches nodes).
  - Data communication (over the overlay network) between Spokes is relayed via the Hub.
  - Multiple Hubs may exists to provide redundancy.
- Spoke-Spoke
  - Individual branch office nodes can dynamically initiate tunnel connections between each other, bypassing the Hub node.
  - Data communication (over the overlay network) can be direct between Spokes.
  - Dynamic IGP routing protocols may operate between Spoke and Hubs, but not between Spokes.
  - No interoperability with non-Cisco IOS routers. (?)

IPSec

- Framework of security protocols and algorithms used to secure data at the network layer
- Authentication Header (AH)
  - Ensures data integrity
  - Does not provide confidentiality
  - Provides origin authentication
  - Uses Keyed-hash mechanisms
- Encapsulating Security Payload (ESP)
  - Provides data confidentiality (encryption)
  - Data Integrity
  - Does not protect IP header
- AH and ESP use symmetric secret key algorithms, although public key algorithms are feasible

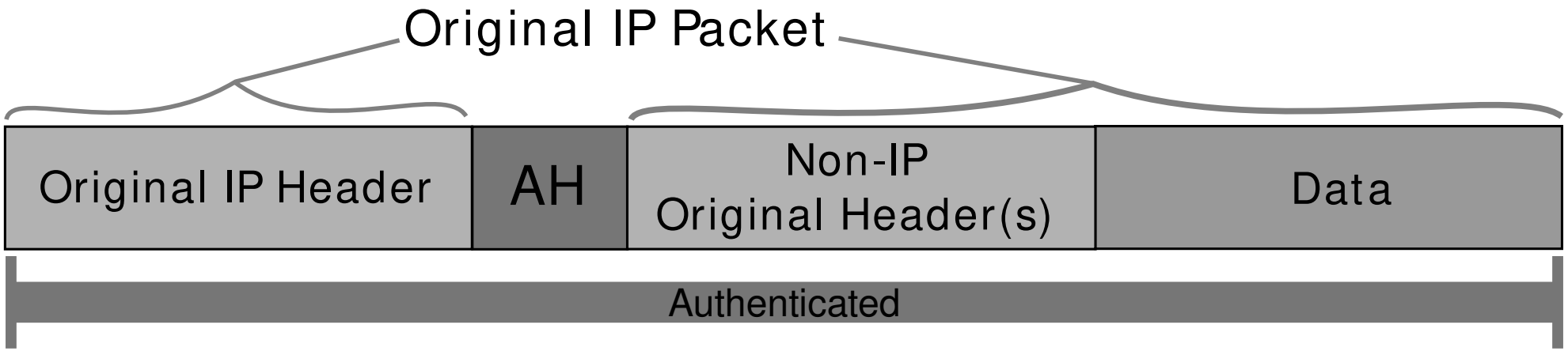
IPSec Modes

- Tunnel
  - IPSec gateways provide IPSec services to other hosts in peer-to-peer tunnels
  - End-hosts are not aware of IPSec being used to protect their traffic
  - IPSec gateways provide transparent protection over untrusted networks
- Transport
  - Each end host does IPSec encapsulation of its own data, host-to-host.
  - IPSec has to be implemented on end-hosts
  - The application endpoint must also be the IPSec endpoint

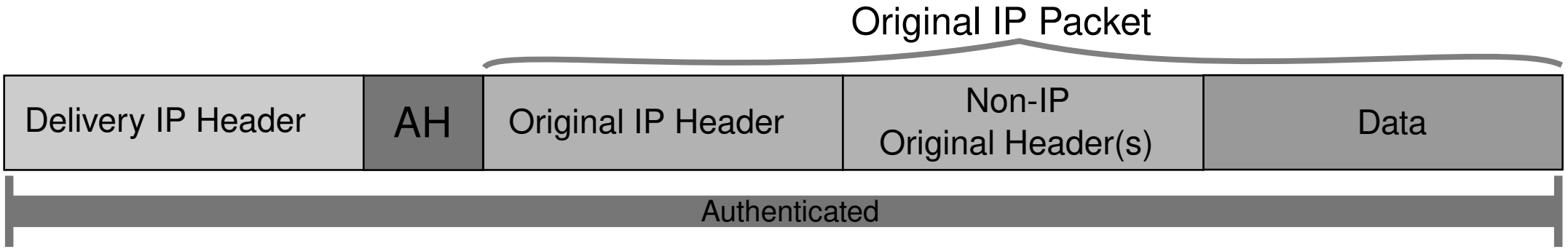


IPSec - AH header placement

- Transport mode

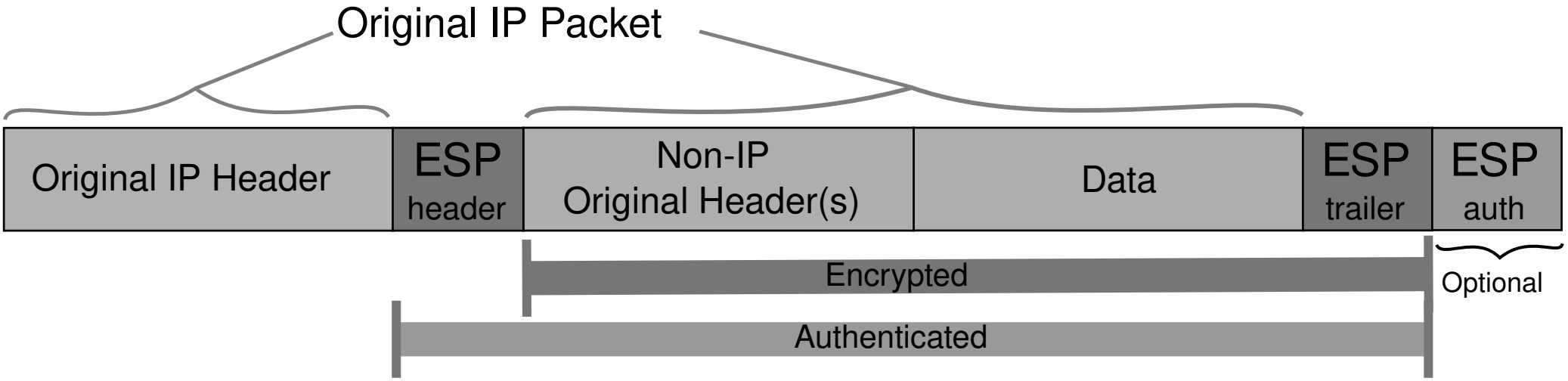


- Tunnel mode

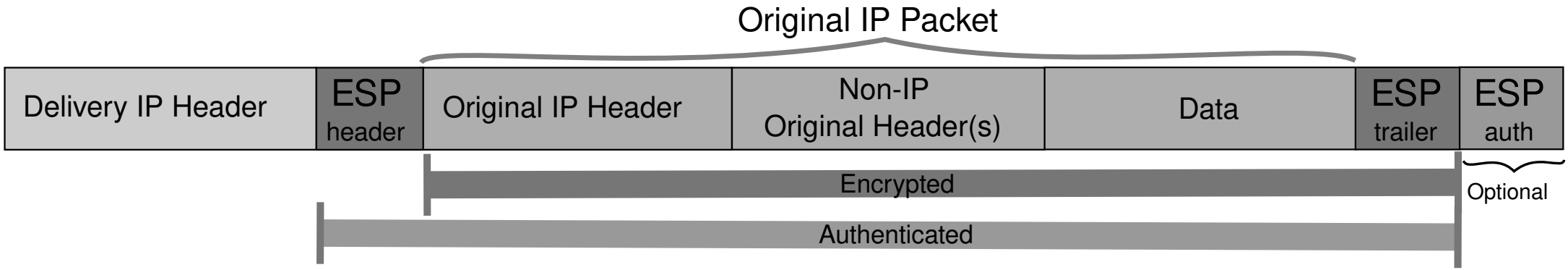


IPSec - ESP header placement

- Transport mode

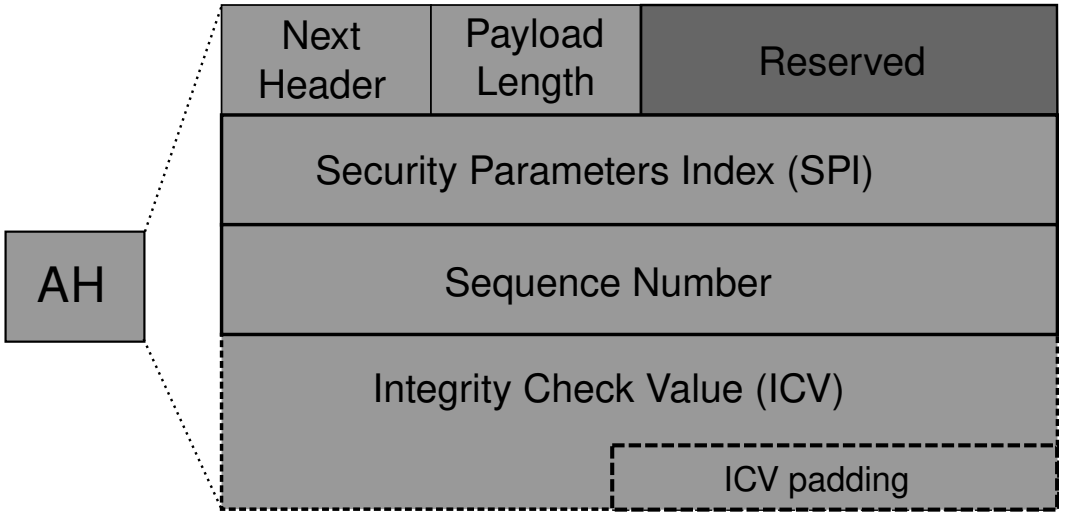


- Tunnel mode



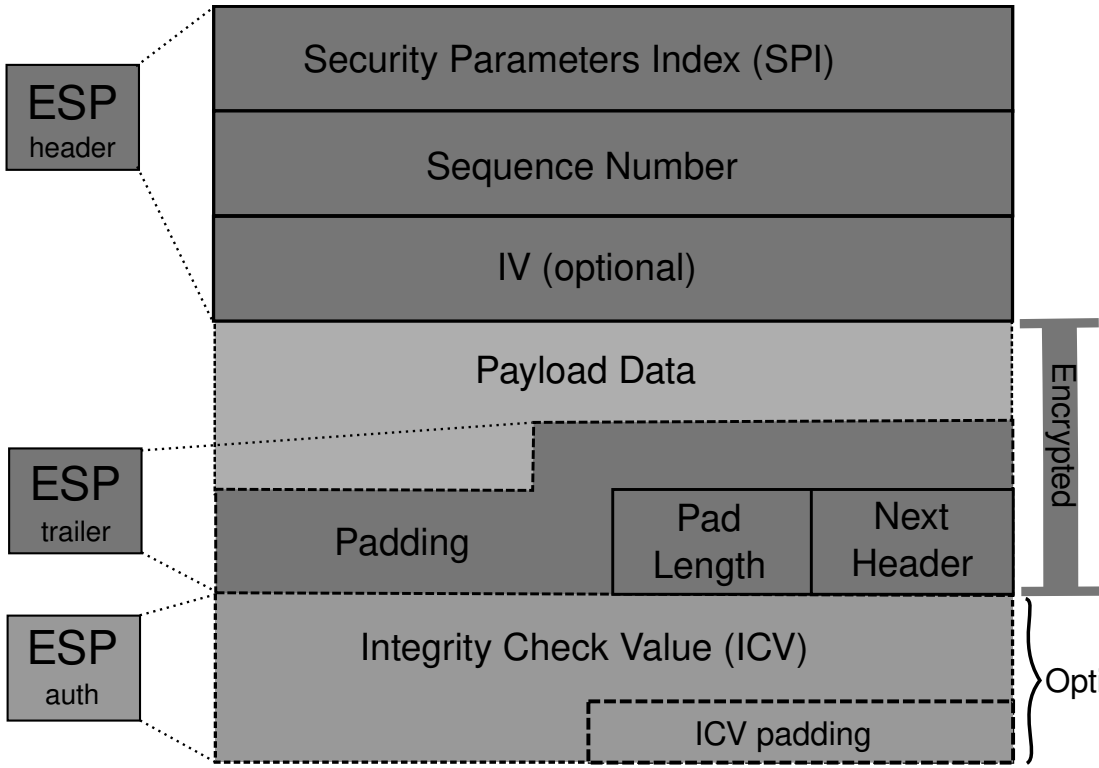
IPsec AH Header

- Contains five mandatory fields:
  - The Next Header field is an 8-bit field that identifies the type of the next payload after the AH.
  - The Payload Length is an 8-bit field specifying the length of the header (excluding the first 8 bytes) in 4-byte units.
  - The SPI field contains the negotiated outbound IPsec SPI and is used by the remote peer to identify the SA to which the packet belongs.
  - The Sequence Number field is a 32-bit field that contains a counter value that increases by one for each sent packet (using the same outbound IPsec SA).
  - The ICV field has a variable length (multiple of 32 bits) that contains the output of the authentication hash function (or HMAC based on symmetric encryption algorithms) applied to data/headers under protection.
    - May include padding to ensure that the overall length of the AH header is a multiple of 32 bits in IPv4 or 64 bits in IPv6.



IPsec ESP Header and Trailer

- Contain five mandatory fields:
  - The SPI field contains the negotiated outbound IPsec SPI and is used by the remote peer to identify the SA to which the packet belongs.
  - The Sequence Number field is a 32-bit field that contains a counter value that increases by one for each sent packet (using the same outbound IPsec SA).
  - The Padding field may contain 0 to 255 zero-bytes to guarantee: (i) a specific payload size imposed by the encryption algorithm (e.g., size multiple of the block cipher size), and (ii) that the Pad Length and Next header fields are right aligned within a 4-byte word.
  - The Pad Length is an 8-bit field that indicates the number of padding bytes in the Padding field.
  - The Next Header is an 8-bit field that identifies the type of data contained in the payload data.
- May contain two optional fields:
  - When the encryption algorithm requires an explicit Initialization Vector (IV), this value is sent using the IV field.
    - Some algorithm modes combine encryption and integrity into a single operation.
  - The ICV field field has a variable length that contains the output of the authentication hash function (or HMAC based on symmetric encryption algorithms) applied to ESP header, Payload Data, and ESP trailer fields.
    - The ICV field may include padding.



IPSec - Security Associations

- SAs represent a policy contract between two peers or hosts
- Describe how the peers will use IPSec security services to protect network traffic
- An SA contains the following security parameters:
  - Authentication/encryption algorithm, key length and other encryption parameters (e.g. key lifetime, ...)
  - Session keys for authentication, or HMACs, and encryption, which can be entered manually or negotiated automatically
  - A specification of network traffic to which the SA will be applied (e.g. IP traffic or only TELNET sessions)
  - IPSec AH or ESP encapsulation protocol and tunnel or transport mode

Establishing SA and Cryptographic Keys

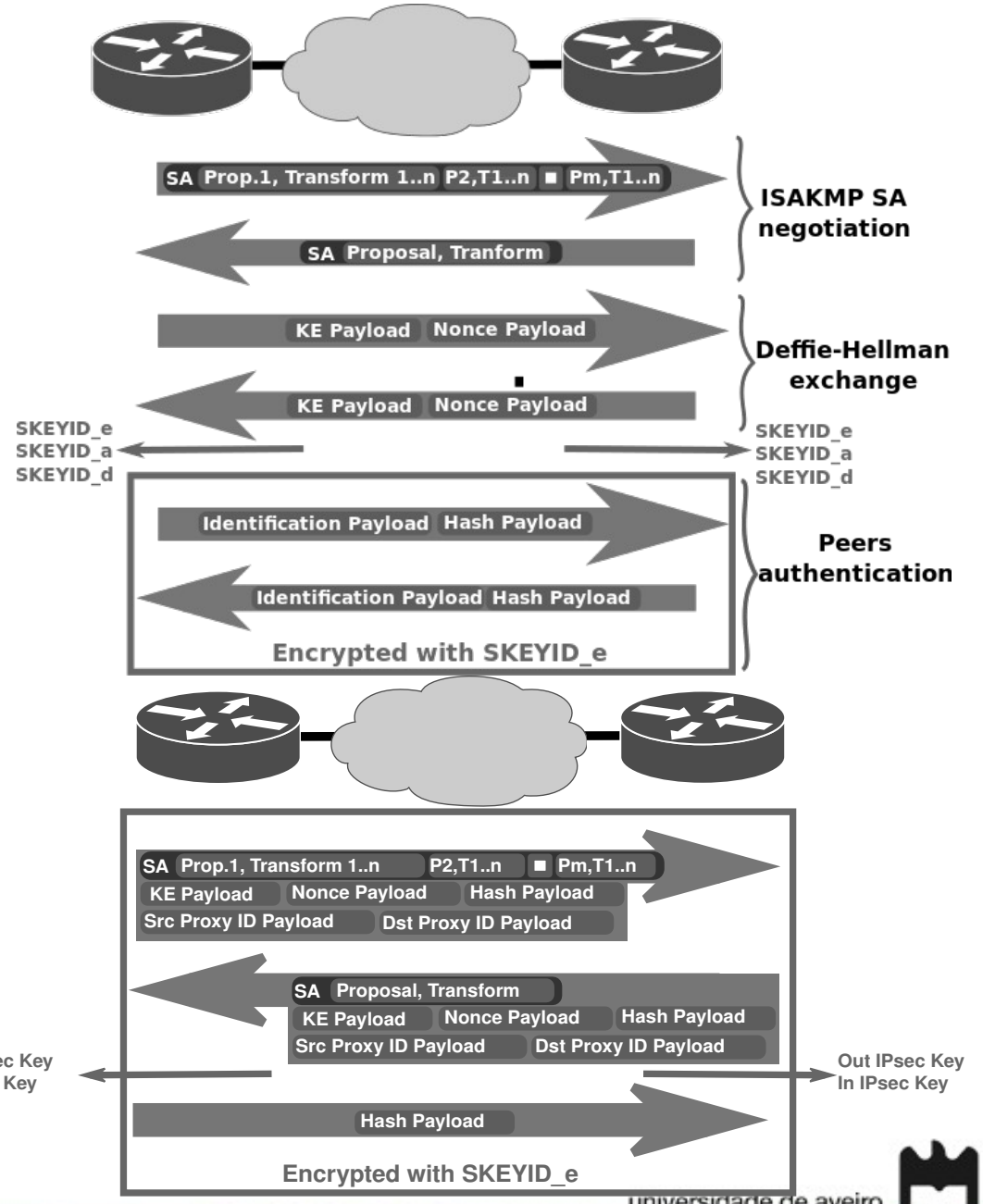
- ISAKMP - Internet Security Association and Key Management Protocol
  - Used to establishing Security Associations (SA) and cryptographic keys
  - Separate the details of security association management (and key management) from the details of key exchange
  - Provides a framework for authentication and key exchange but does not define them
- Oakley Key Determination Protocol
  - Key-agreement protocol
  - Allows authenticated peers to exchange keying material across an insecure connection
  - Uses Diffie-Hellman
- SKEME
  - Key exchange protocol
- IKE - Internet Key Exchange
  - Is a hybrid protocol
  - Uses part of Oakley and part of SKEME in conjunction with ISAKMP

IKE/ISAKMP and IPsec

- Enhances IPSec by providing additional features and flexibility
- Provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations
- The IKE tunnel protects the SA negotiations. After the SAs are in place, IPSec protects data transference
- Advantages
  - Eliminates the need to manually specify IPSec security parameters at both peers
  - Allows administrators to specify a lifetime for the IPSec security association
  - Allows encryption keys to change during IPSec sessions
  - Allows IPSec to provide anti-replay services
  - Permits certification authority (CA) support for a manageable, scalable IPSec implementation
  - Allows dynamic authentication of peers
- IKE/ISAKMP provides three methods for two-way authentication:
  - Pre-shared key (PSK),
  - Digital signatures (RSA-SIG),
  - Public key encryption (RSA-ENC).

ISAKMP and IPsec – Phases/Modes

- ISAKMP modes control an efficiency versus security tradeoff during initial key exchange
- Phase 1
  - Peer agree on a set of parameters to be used to authenticate peers and to encrypt a portion of the phase 1 exchanges and all of phase 2 exchanges, authenticate peers, and generate keys to be used as generating keying material.
  - Main mode
    - Requires six packets back and forth
    - Provides complete security during the establishment of an IPsec connection
    - Aggressive mode is an alternative to main mode
      - Uses half the exchanges, but provides less security because some information is transmitted in cleartext
- Phase 2 - Quick mode
  - Peers negotiate and agree on parameters required to establish a fully functional IPsec communication service.



IPsec Packet Exchange

No.	Time	Source	Destination	Protocol	Length	Info
12	12.259744000	2001:a:a::2	2001:a:a::1	ISAKMP	146	Identity Protection (Main Mode)
13	12.293700000	2001:a:a::1	2001:a:a::2	ISAKMP	146	Identity Protection (Main Mode)
14	12.330320000	2001:a:a::2	2001:a:a::1	ISAKMP	298	Identity Protection (Main Mode)
15	12.364351000	2001:a:a::1	2001:a:a::2	ISAKMP	318	Identity Protection (Main Mode)
16	12.481540000	2001:a:a::2	2001:a:a::1	ISAKMP	170	Identity Protection (Main Mode)
17	12.496192000	2001:a:a::1	2001:a:a::2	ISAKMP	138	Identity Protection (Main Mode)
18	12.542122000	2001:a:a::2	2001:a:a::1	ISAKMP	250	Quick Mode
19	12.556571000	2001:a:a::1	2001:a:a::2	ISAKMP	250	Quick Mode
20	12.582568000	2001:a:a::2	2001:a:a::1	ISAKMP	114	Quick Mode
21	15.425134000	2001:a:a::2	2001:a:a::1	ESP	322	ESP (SPI=0xb26693bc)
22	15.440166000	2001:a:a::1	2001:a:a::2	ESP	202	ESP (SPI=0x328b3017)

```
▷ Frame 21: 322 bytes on wire (2576 bits), 322 bytes captured (2576 bits) on interface 0
▷ Ethernet II, Src: c2:04:62:06:00:00 (c2:04:62:06:00:00), Dst: ca:06:73:90:00:08 (ca:06:73:90:00:08)
▷ Internet Protocol Version 6, Src: 2001:a:a::2 (2001:a:a::2), Dst: 2001:a:a::1 (2001:a:a::1)
▽ Encapsulating Security Payload
    ESP SPI: 0xb26693bc (2993066940)
    ESP Sequence: 10
```

ISAKMP (phase 1) First Message

```
▷ Internet Protocol Version 4, Src: 200.2.2.2 (200.2.2.2), Dst: 200.1.1.1 (200.1.1.1)
▷ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
▽ Internet Security Association and Key Management Protocol
   Initiator SPI: 06ba66b161c0b75d
   Responder SPI: 0000000000000000
   Next payload: Security Association (1)
  ▷ Version: 1.0
   Exchange type: Identity Protection (Main Mode) (2)
  ▷ Flags: 0x00
   Message ID: 0x00000000
   Length: 204
  ▽ Type Payload: Security Association (1)
     Next payload: Vendor ID (13)
     Payload length: 96
     Domain of interpretation: IPSEC (1)
    ▷ Situation: 00000001
    ▽ Type Payload: Proposal (2) # 1
       Next payload: NONE / No Next Payload  (0)
       Payload length: 84
       Proposal number: 1
       Protocol ID: ISAKMP (1)
       SPI Size: 0
       Proposal transforms: 2
      ▷ Type Payload: Transform (3) # 1
      ▷ Type Payload: Transform (3) # 2
  ▷ Type Payload: Vendor ID (13) : RFC 3947 Negotiation of NAT-Traversal in the IKE
  ▷ Type Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-07
  ▷ Type Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-03
  ▷ Type Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-02\n
```

ISAKMP (phase 1) Second Message

```
▷ Internet Protocol Version 4, Src: 200.1.1.1 (200.1.1.1), Dst: 200.2.2.2 (200.2.2.2)
▷ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
▽ Internet Security Association and Key Management Protocol
   Initiator SPI: 06ba66b161c0b75d
   Responder SPI: 48aa62bdcb19e9e3
   Next payload: Security Association (1)
 ▷ Version: 1.0
   Exchange type: Identity Protection (Main Mode) (2)
 ▷ Flags: 0x00
   Message ID: 0x00000000
   Length: 104
 ▽ Type Payload: Security Association (1)
     Next payload: Vendor ID (13)
     Payload length: 56
     Domain of interpretation: IPSEC (1)
   ▷ Situation: 00000001
   ▽ Type Payload: Proposal (2) # 1
       Next payload: NONE / No Next Payload  (0)
       Payload length: 44
       Proposal number: 1
       Protocol ID: ISAKMP (1)
       SPI Size: 0
       Proposal transforms: 1
     ▷ Type Payload: Transform (3) # 1
▷ Type Payload: Vendor ID (13) : RFC 3947 Negotiation of NAT-Traversal in the IKE
```

ISAKMP (phase 1) Third and Fourth Messages

```
▷ Internet Protocol Version 4, Src: 200.2.2.2 (200.2.2.2), Dst: 200.1.1.1
▷ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
▽ Internet Security Association and Key Management Protocol
   Initiator SPI: 06ba66b161c0b75d
   Responder SPI: 48aa62bdcb19e9e3
   Next payload: Key Exchange (4)
 ▷ Version: 1.0
   Exchange type: Identity Protection (Main Mode) (2)
 ▷ Flags: 0x00
   Message ID: 0x00000000
   Length: 276
 ▽ Type Payload: Key Exchange (4)
     Next payload: Nonce (10)
     Payload length: 132
     Key Exchange Data: 6b90894c1593b8dddda8d321a05af807
 ▽ Type Payload: Nonce (10)
     Next payload: Vendor ID (13)
     Payload length: 24
     Nonce DATA: 21edc1d7ee9a9a51d9d8a0fccc1012ff9d58a348
 ▷ Type Payload: NAT-D (RFC 3947) (20)
 ▷ Type Payload: NAT-D (RFC 3947) (20)
```

```
▷ Internet Protocol Version 4, Src: 200.1.1.1 (200.1.1.1), Dst: 200.2.2.2
▷ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
▽ Internet Security Association and Key Management Protocol
   Initiator SPI: 06ba66b161c0b75d
   Responder SPI: 48aa62bdcb19e9e3
   Next payload: Key Exchange (4)
 ▷ Version: 1.0
   Exchange type: Identity Protection (Main Mode) (2)
 ▷ Flags: 0x00
   Message ID: 0x00000000
   Length: 296
 ▽ Type Payload: Key Exchange (4)
     Next payload: Nonce (10)
     Payload length: 132
     Key Exchange Data: 820d0eafec6260bc958a60d1d086e6ec823032774f16c316...
 ▽ Type Payload: Nonce (10)
     Next payload: Vendor ID (13)
     Payload length: 24
     Nonce DATA: 0f37423fb10f422983fcf0d9dcab26a5b8be59aa
 ▷ Type Payload: NAT-D (RFC 3947) (20)
 ▷ Type Payload: NAT-D (RFC 3947) (20)
```

ISAKMP (phase 1) Fifth and Sixth Messages

```
▷ Internet Protocol Version 4, Src: 200.2.2.2 (200.2.2.2), Dst: 200.1.1.1
▷ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
▽ Internet Security Association and Key Management Protocol
   Initiator SPI: 06ba66b161c0b75d
   Responder SPI: 48aa62bdcb19e9e3
   Next payload: Identification (5)
 ▷ Version: 1.0
   Exchange type: Identity Protection (Main Mode) (2)
 ▷ Flags: 0x01
   Message ID: 0x00000000
   Length: 92
   Encrypted Data (64 bytes)
```

```
▷ Internet Protocol Version 4, Src: 200.1.1.1 (200.1.1.1), Dst: 200.2.2.2
▷ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
▽ Internet Security Association and Key Management Protocol
   Initiator SPI: 06ba66b161c0b75d
   Responder SPI: 48aa62bdcb19e9e3
   Next payload: Identification (5)
 ▷ Version: 1.0
   Exchange type: Identity Protection (Main Mode) (2)
 ▷ Flags: 0x01
   Message ID: 0x00000000
   Length: 68
   Encrypted Data (40 bytes)
```

ISAKMP (phase 2) Message

```
▷ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
▽ Internet Security Association and Key Management Protocol
    Initiator SPI: 06ba66b161c0b75d
    Responder SPI: 48aa62bdcb19e9e3
    Next payload: Hash (8)
  ▷ Version: 1.0
    Exchange type: Quick Mode (32)
  ▷ Flags: 0x01
    Message ID: 0x5277ae21
    Length: 220
    Encrypted Data
```

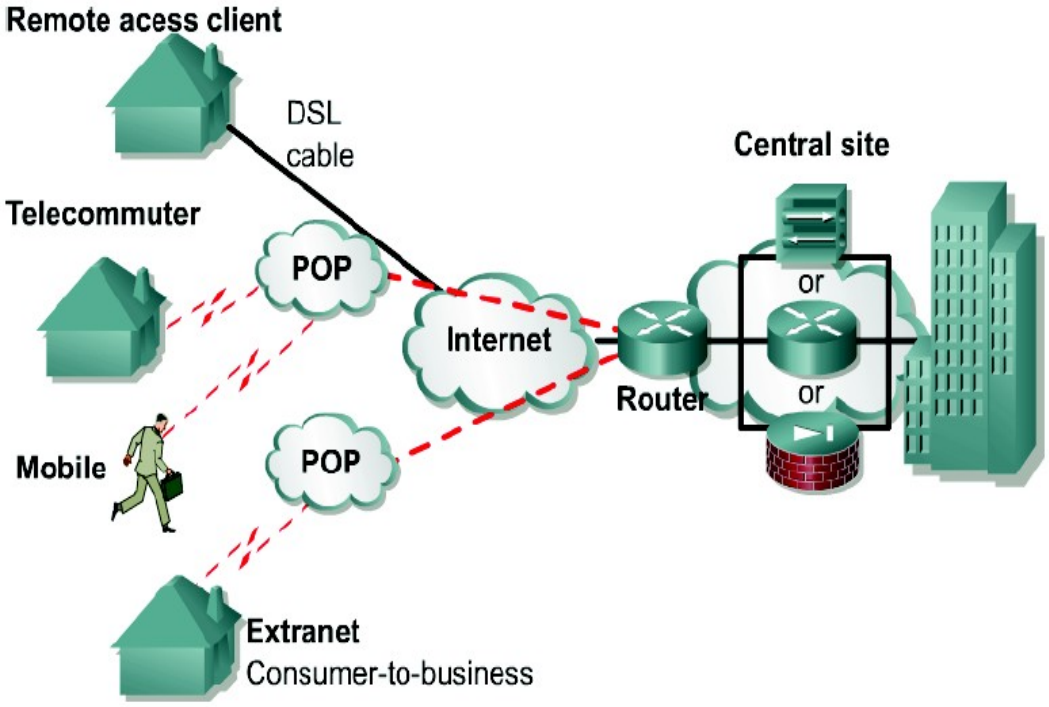
IPsec NAT Transversal

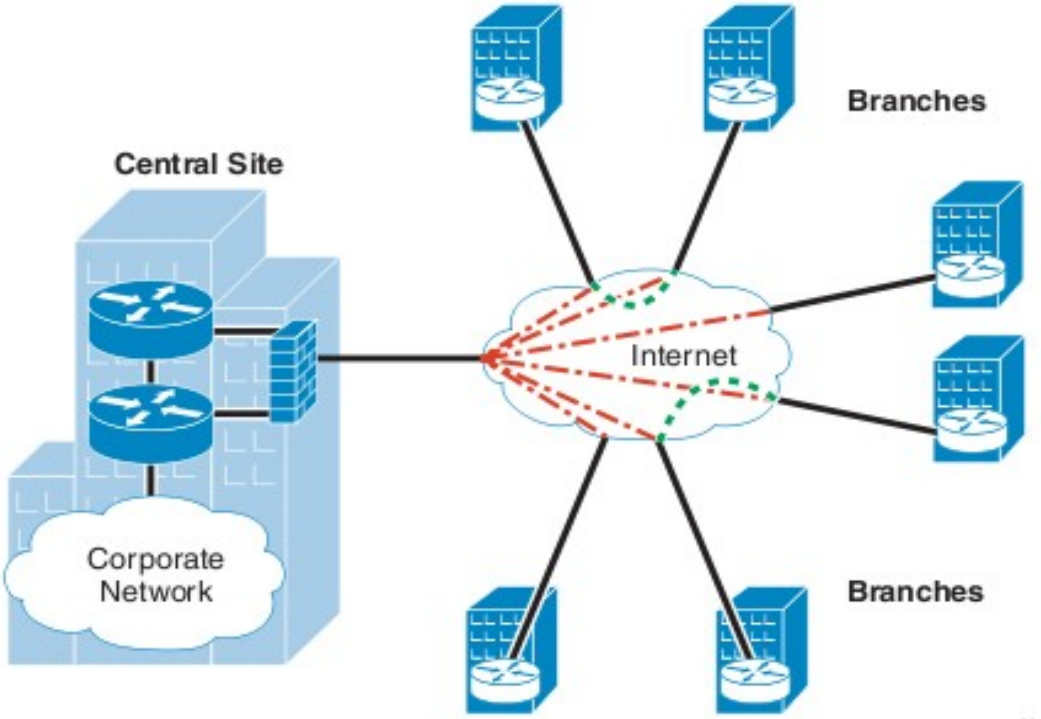
- NAT/PAT incompatibilities with IPsec
  - AH header incorporates the IP source and destination addresses in the keyed message integrity check. ESP is not an issue.
  - TCP and UDP checksums can be updated because are protected by IPsec.
  - IP addresses may be used as identifiers in Internet Key Exchange to determine credentials.
- During the ISAKMP IPsec first phase hosts (when configured and suported) detect that NAT transversal must be activated.
  - Subsequent ISAKMP first phase and second phase packets are encapsulated in UDP packets.
    - Usually port UDP 4500.
  - Original IP address are sent as NAT-OA (NAT Original Address) payloads of the ISAKMP.

Virtual Private Networks (VPN)

VPN - Virtual Private Networks

- Is an encrypted connection between private networks over a public network





- Remote Access VPN
- Site-to-Site VPN

VPN types

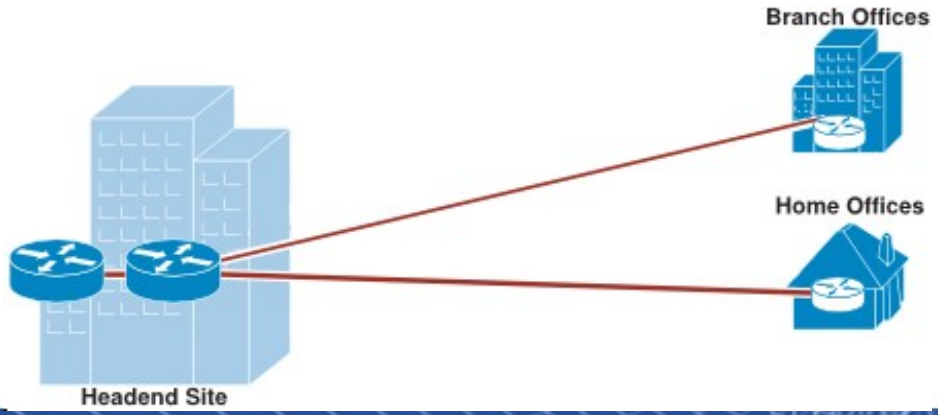
- Remote Access VPN
  - PPTP
  - L2TP/IPsec
  - SSL/TLS VPN
    - Web VPN (client-less SSL VPN) – VPN client can be a standard browser
  - SSH VPN
  - Open VPN
- Site-to-Site VPN
  - IPsec VPN
    - With static or dynamic configuration
  - IPsec + GRE VPN
    - Dynamic Multipoint VPN

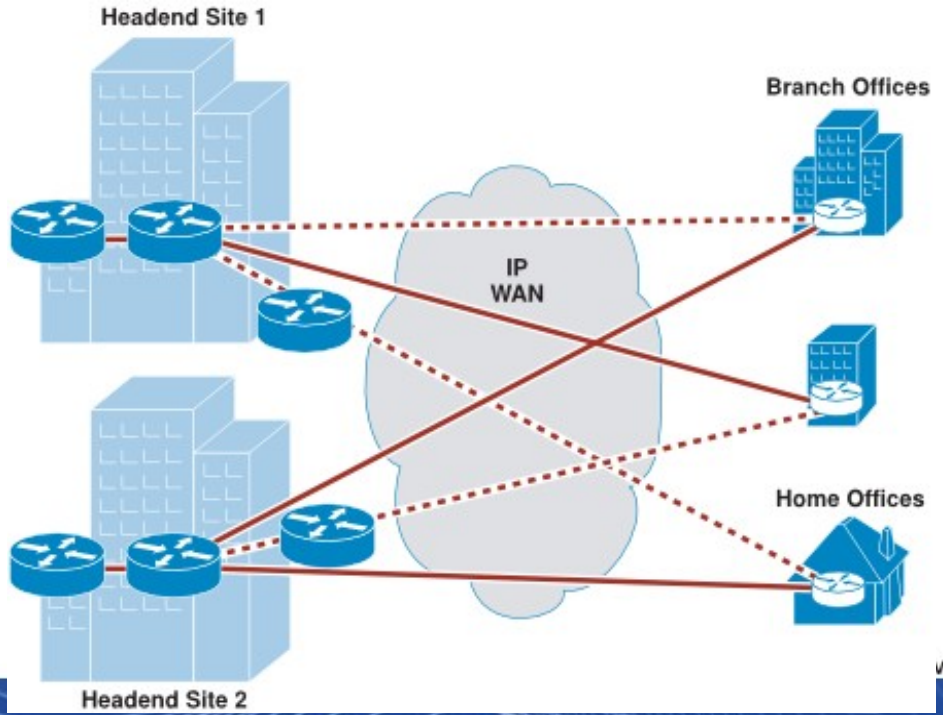
Variants of Site-to-Site IPsec VPN

- IPsec tunnels with static configuration
  - Requires the knowledge of all peers (IP addresses and security parameters)
  - High configuration overhead
- IPsec tunnels with dynamic configuration (at the headend/hub)
  - Hub + spokes configuration
  - Generic configuration at the headend/hub
  - Easy to add new spokes

➔ A basic IPsec tunnel can't protect multicast traffic.

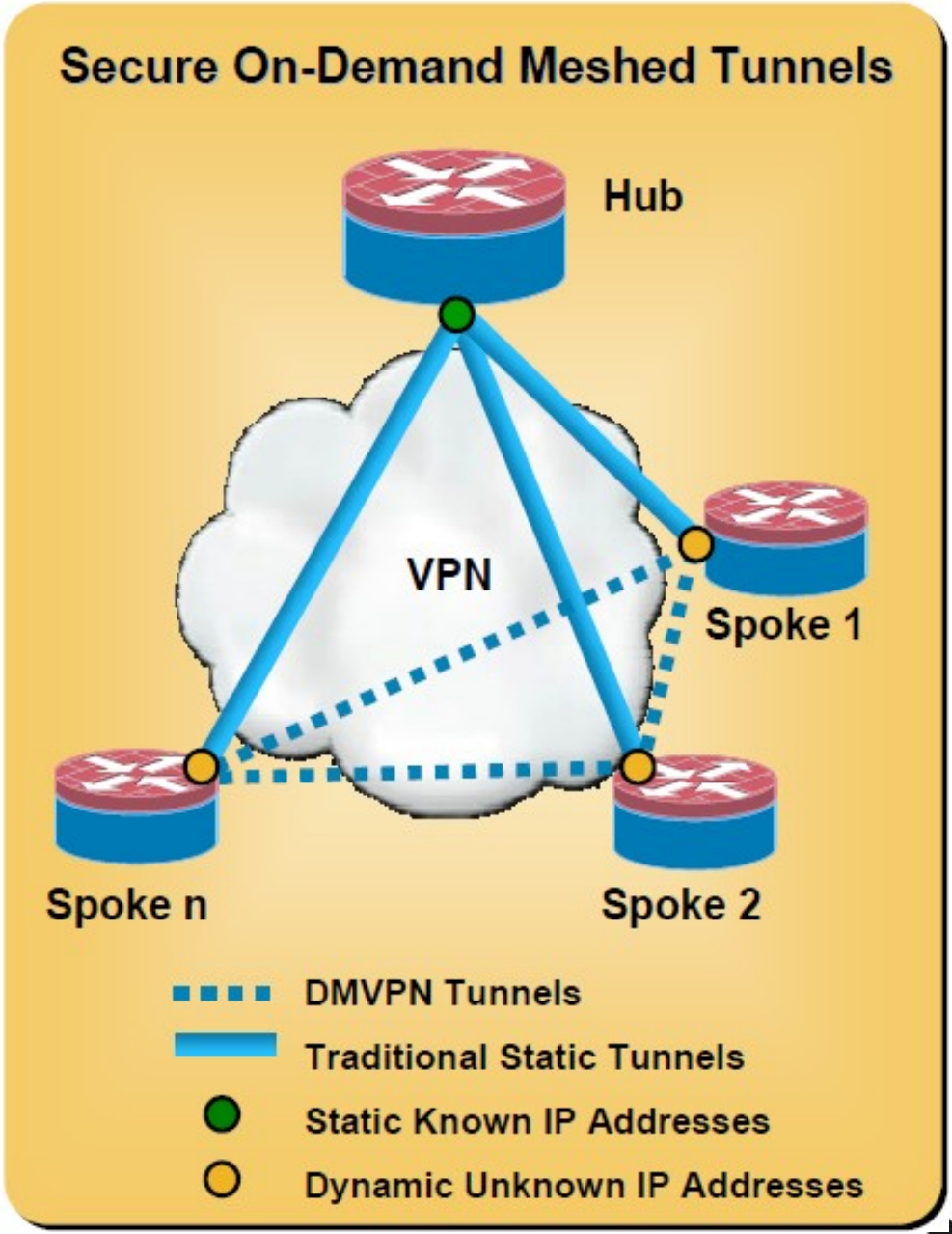
- IPsec + GRE tunnels
  - Generic Routing Encapsulation (GRE) allows the protection of multicast traffic over IPsec
- Dynamic Multipoint VPN (DMVPN)



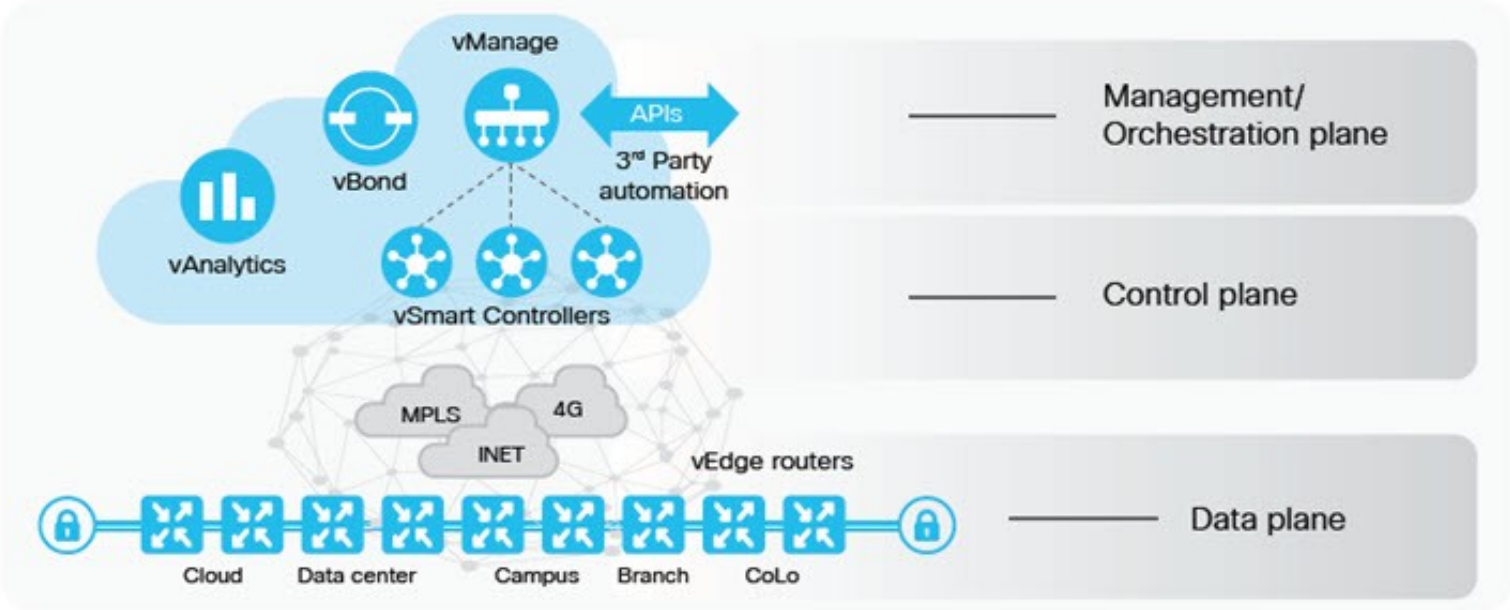


Dynamic Multipoint VPN

- Relies on NHRP to create overlay network
- Provides full meshed connectivity with simple configuration of hub and spoke
- Supports dynamically addressed spokes
- Facilitates zero-touch configuration for addition of new spokes
- Features automatic IPsec triggering for building an IPsec tunnel



SD-WAN



- Software Defined WAN
  - Edge Connectivity Abstraction.
  - WAN Virtualization.
  - Policy-Driven, Centralized Management.
  - Elastic Traffic Management.
  - Advantages: Easy deployment and management.
  - Disadvantages: Completely dependence (present and future) on external providers.

Remote Access VPN

- Most common servers/protocols
  - L2TP IPsec
    - IKE+ISAKMP+L2TP
  - OpenVPN
    - SSL
  - Proprietary
    - SSL or IPSec based.
- Authentication
  - Types
    - Pre-shared
    - RADIUS/LDAP
    - RSA with embedded CA
    - RSA with external CA
  - Certificates/Credentials must be distributed securely
    - Web service, SSH, ...

Remote Access VPN - L2TP/IPSec VPN

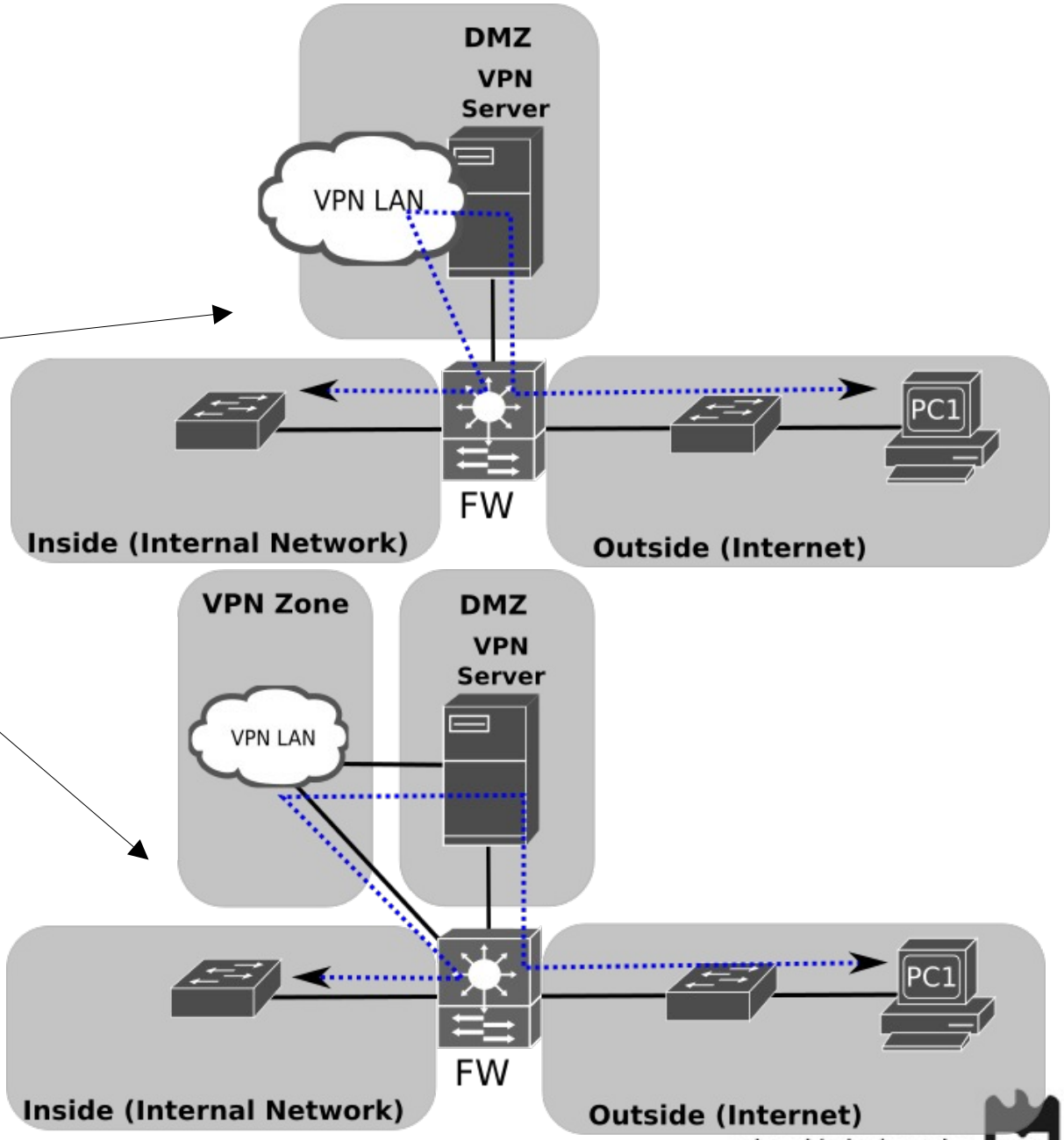
- Authentication can be performed with Digital Certificates (RSA) or with the same PPP authentication mechanisms as PPTP
- Provides data integrity, authentication of origin and replay protection
- Encryption provided by IPSec (ESP protocol)
- Can support multiple, simultaneous tunnels for each user
- Slower performance than PPTP

Other Remote Access VPN types

- SSL/TLS VPN
  - SSL/TLS protocol handles the VPN tunnel creation
  - SSL/TLS is much easier to implement than IPSec and provides a simple and well-tested platform
  - RSA handshake (or DH) is used exactly as IKE in IPSec
- SSH VPN
  - VPN over a SSH connection
  - SSH tunneling - port forwarding
- OpenVPN
  - Implements a SSL/TLS VPN
  - Allows PSK, certicate, and login/password based authentication
  - Encryption provided by OpenSSL (can use all ciphers available)
  - Compatible with dynamic and NAT addresses

Remote VPN Network Integration

- Server deployed in Firewalls.
- Server in DMZ.
  - Traffic routed back to the firewall using the same zone.
  - Traffic routed back to the firewall using the a different network interface and zone.
  - Traffic routed directly to private zone.
    - Breaks zone concept.



Integration with Flow Control

- Service/protocol rules
  - OpenVPN
    - Used UDP port.
      - Usually port UDP 1194.
  - IPsec
    - UDP port 500 for IKE.
    - IP protocol number 50 (ESP).
      - IP protocol number 51 (AH).
    - UDP port 4500 for NAT traversal.
  - L2TP
    - UDP port 1701.
    - Exception may not be required when L2TP is encapsulated within IPsec packets.
- User flows' rules
  - Remote users are assigned a IP network address.
  - Flow control based on IP address or zone.

Intrusion Detection and Prevention

Segurança em Redes de Comunicações

Mestrado em Cibersegurança

Mestrado em Engenharia de Computadores e Telemática

DETI-UA

universidade de aveiro

deti.ua.pt

Intrusion Detection and Prevention

- Intrusion Detection Systems (IDS)
  - Monitoring and identifying unauthorized system access or manipulation.
  - Analyzes information from multiple sources (computers, servers, services, and network traffic).
  - Identifies:
    - Intrusions, attacker outside of the organization;
    - Misuse, wrong behavior from a licit user/service.
  - Does not block/prevent intrusion.
  - Signals an alarm for:
    - Human analysis and intervention;
    - Automatic threat responses by firewalls or centralized management systems.
- Intrusion Prevention Systems (IPS)
  - At network level blocks traffic;
  - At host level kills processes, quarantines a file, blocks device access, etc...

Host-Based vs. Network-Based

- To protect specific servers or user devices the IDS/IPS is deployed at the host level.
  - Monitors traffic, processes, files' access, devices' access and data flows, memory allocations, physical device characteristics (temperature, power consumption, movement, etc...).
  - Nowdays called Endpoint Detection and Response (EDR).
- To protect an organization (all devices and services) the IDS/IPS is deploy at the network level.
  - Monitors traffic at the packet and flow levels. May monitor network at the physical level (radio, electric and optical signals).
  - Deployed at multiple network points:
    - Internet and WAN accesses;
    - Inter-zone communication links;
    - Wireless.

Signature vs. Anomaly Based

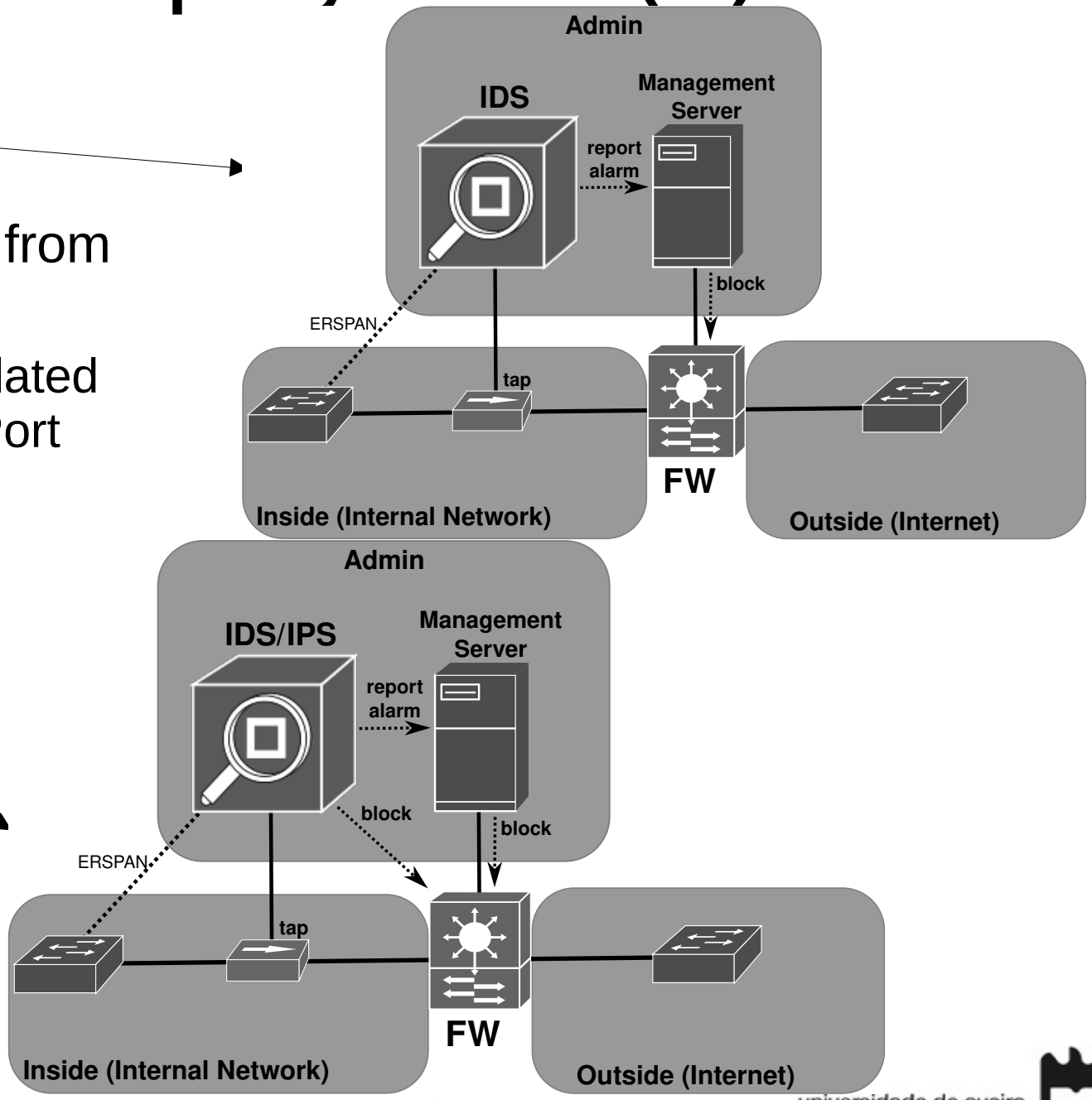
- Intrusions are detected based on two different approaches:
  - Signature based:
    - Monitored data compared to preconfigured and predetermined attack patterns known as signatures;
    - Attacks have distinct known signatures;
    - Signatures must be constantly updated to mitigate emerging threats.
    - Signatures may contain:
      - Individual packet header values or binary data patterns,
      - Sequence of packets with specific characteristics within the same flow, or
      - Set of data flows (data stream) with specific characteristics (of flows or transmitted packets/data).
  - Anomaly based:
    - Establishes a behavior baseline (profile) and detected deviation from that profile;
    - May rely only of high-level systems or network statistics, or include multiple data sources;
    - May be based on predefined rules or on AI models.

Endpoint Detection and Response (EDR)

- Referred also to as endpoint detection and threat response (EDTR).
- Monitor, record and analyze the activities and events on devices.
- Provide continuous and comprehensive visibility of the devices processes and user activities.
- Enables a direct response to incidents in devices/servers.
- May be fully deployed only on the device, or with an agent on device and external data analyze/storage.

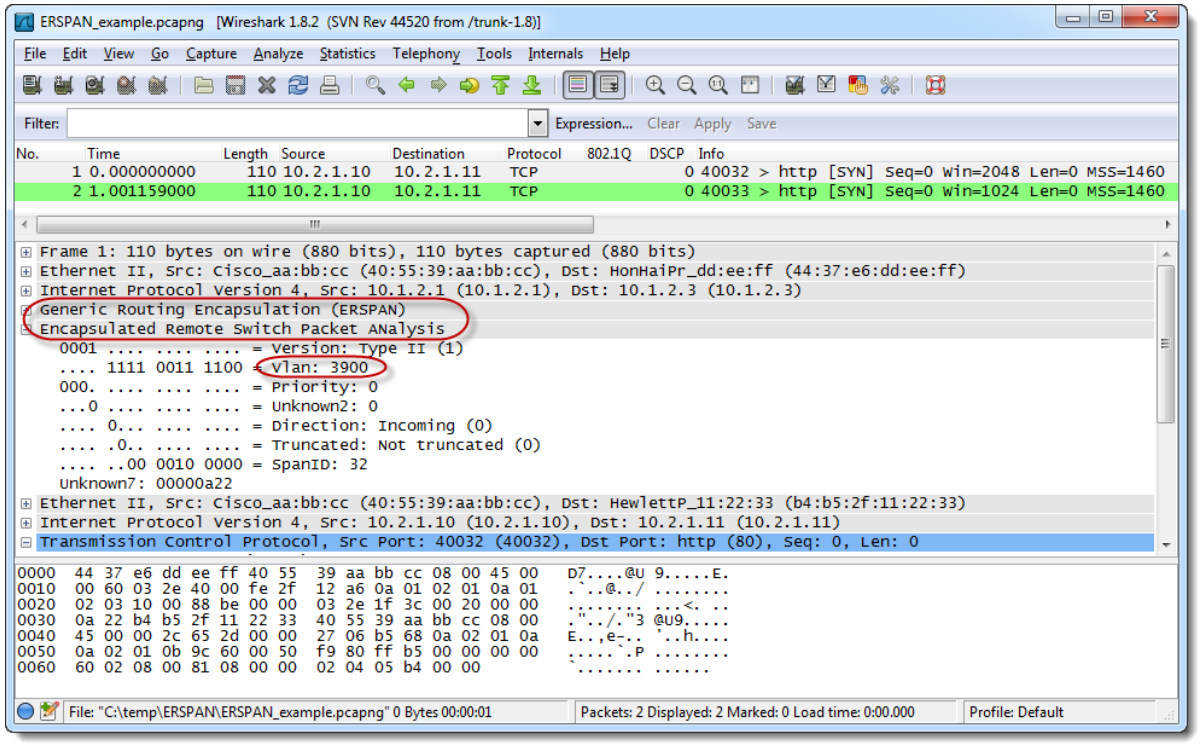
Network Deployment (1)

- IDS
  - Network tap.
  - ERSPAN GRE tunnel from switch.
    - ERSPAN: Encapsulated Remote Switched Port ANalyzer
  - Reports to network management system.
- IPS
  - IDS with firewall integration.



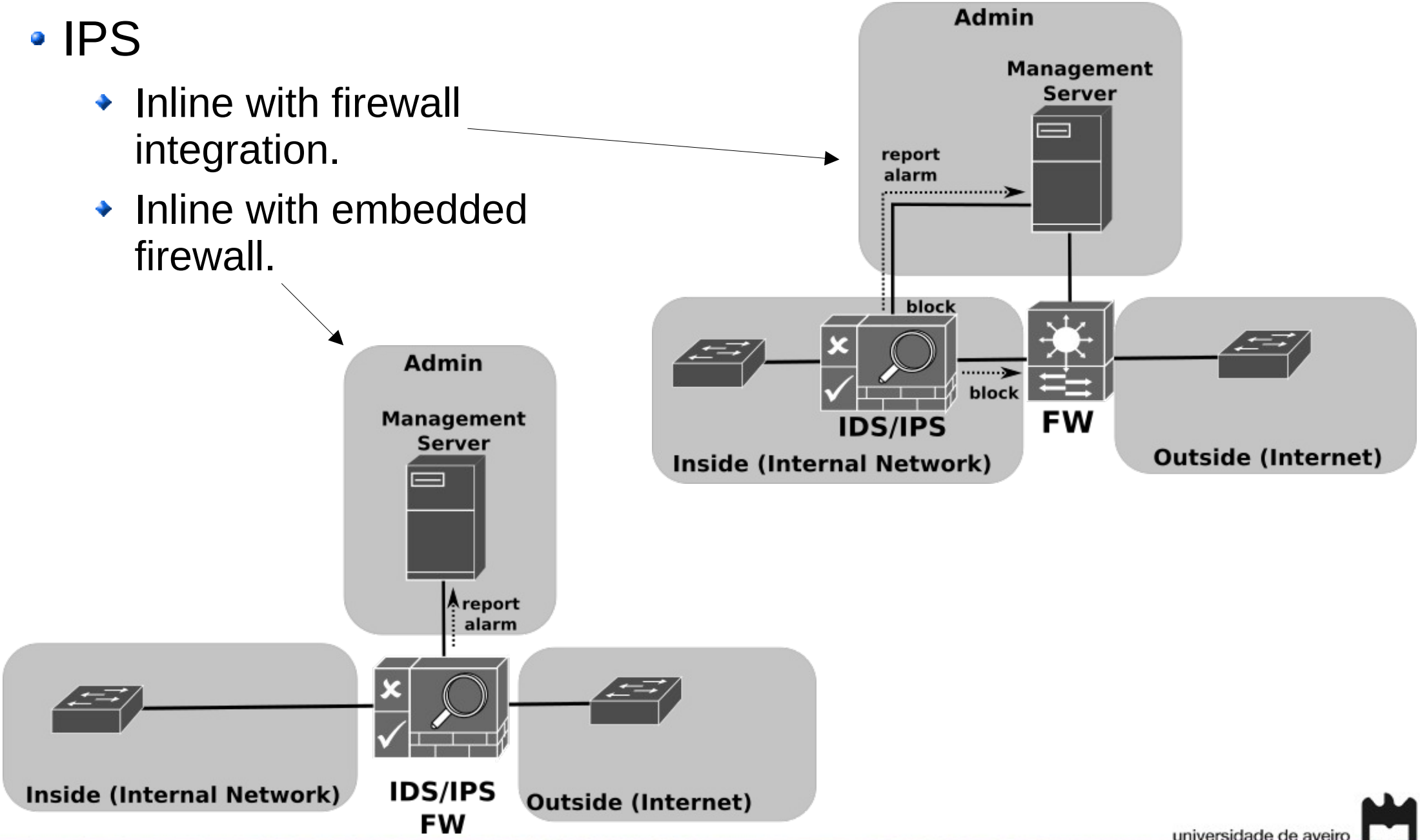
ERSPAN

- Stands for “Encapsulated Remote Switched Port Analyzer”.
- Mirrors traffic from one or more switch ports.
- Sends the mirrored traffic to one or more destinations.
- The traffic is encapsulated in Generic Routing Encapsulation (GRE).



Network Deployment (2)

- IPS
  - Inline with firewall integration.
  - Inline with embedded firewall.



IDS/IPS Actions

- Suricata
  - alert - generate an alert.
  - pass - stop further inspection of the packet.
  - drop - drop packet and generate alert.
  - reject - send RST/ICMP unreach error to the sender of the matching packet.
  - rejectsrc - same as just reject.
  - rejectdst - send RST/ICMP error packet to receiver of the matching packet.
  - rejectboth - send RST/ICMP error packets to both sides of the conversation.
- Snort
  - alert - generate an alert using the selected alert method, and then log the packet.
  - log - log the packet.
  - pass - ignore the packet.
  - drop - block and log the packet.
  - reject - block the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.
  - sdrop - block the packet but do not log it.

Monitoring & SIEM & NOC/SOC

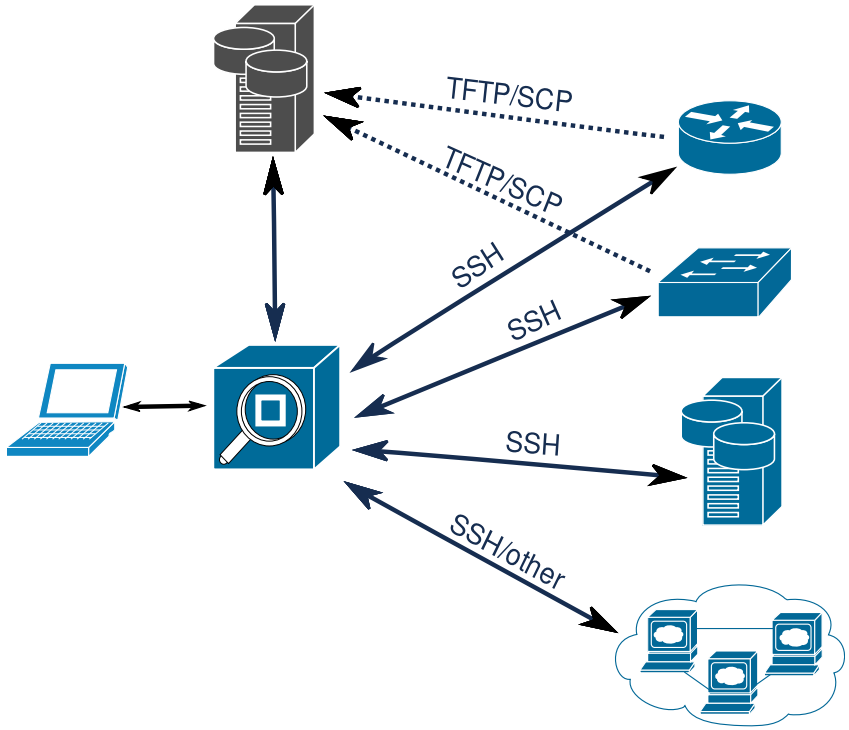
Segurança em Redes de Comunicações

Mestrado em Cibersegurança
Mestrado em Engenharia de Computadores e Telemática
DETI-UA

universidade de aveiro
deti.ua.pt

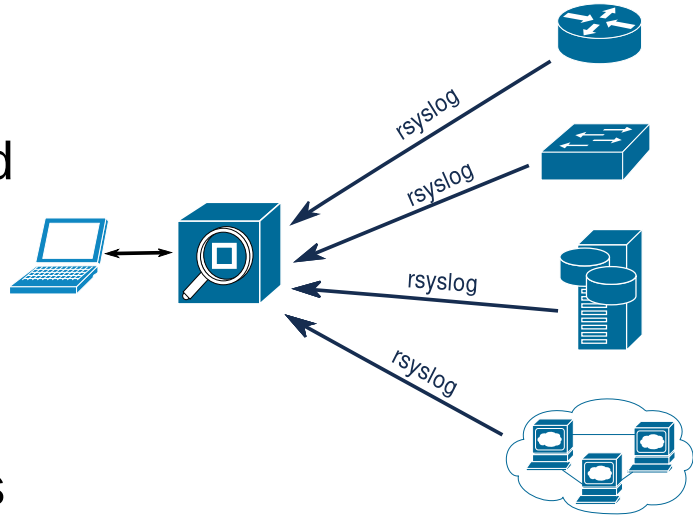
Remote CLI Access

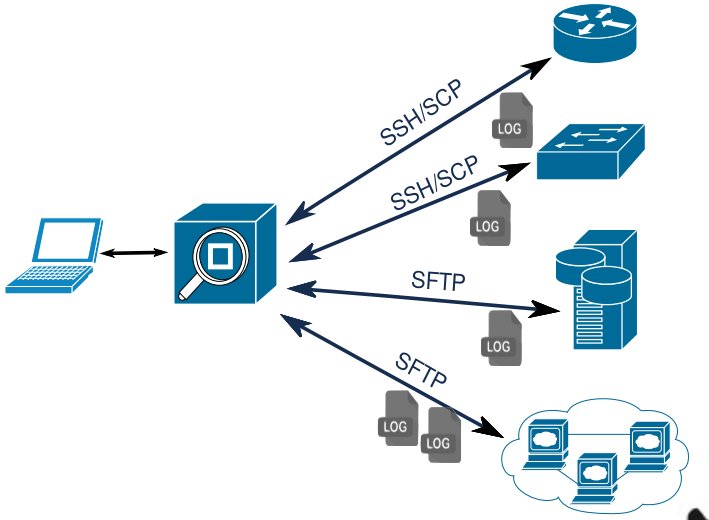
- Using a remote console to devices,
  - Using SSH, telnet (insecure), or proprietary protocols,
  - Retrieve configurations and device's processes status.
  - Devices can also upload configurations to a central point.
    - Using TFTP (insecure) or SFTP/SCP (many devices do not support it).
- Send “show” like CLI commands, retrieve output, parse information.



Log Files Access

- rsyslog
  - Able to accept inputs from a wide variety of services, transform them, and output the results to diverse network destinations.
    - Over TCP and/or SSL/TLS.
  - Timing controlled by monitored node/device.
  - Many post- and cross-processing tasks can be made on the monitored node/device.
- Direct access to log files
  - Using any remote access to remote files.
    - Requires special permissions.
  - SSH/SCP, SFTP, etc...
  - Timing controlled by central point.
  - Requires all heavy post- and cross-processing in a central point.



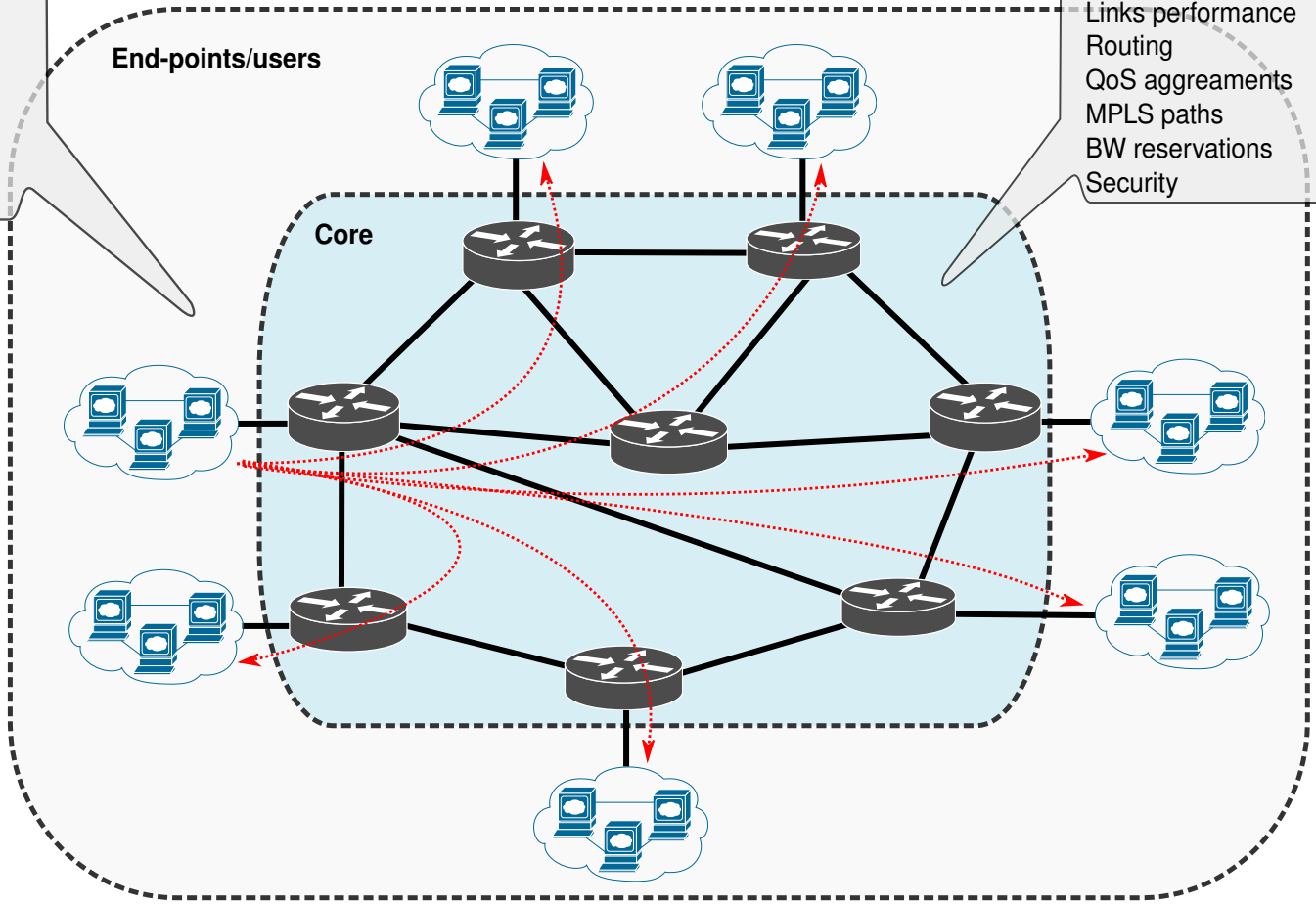


universidade de aveiro

Core and End-to-End Monitoring

End-to-end measurements
- delay
- jitter
- throughput
- losses
- BW reservations
- reserved paths validation

Demands per destination
- global
- per service/app
- per QoS usage



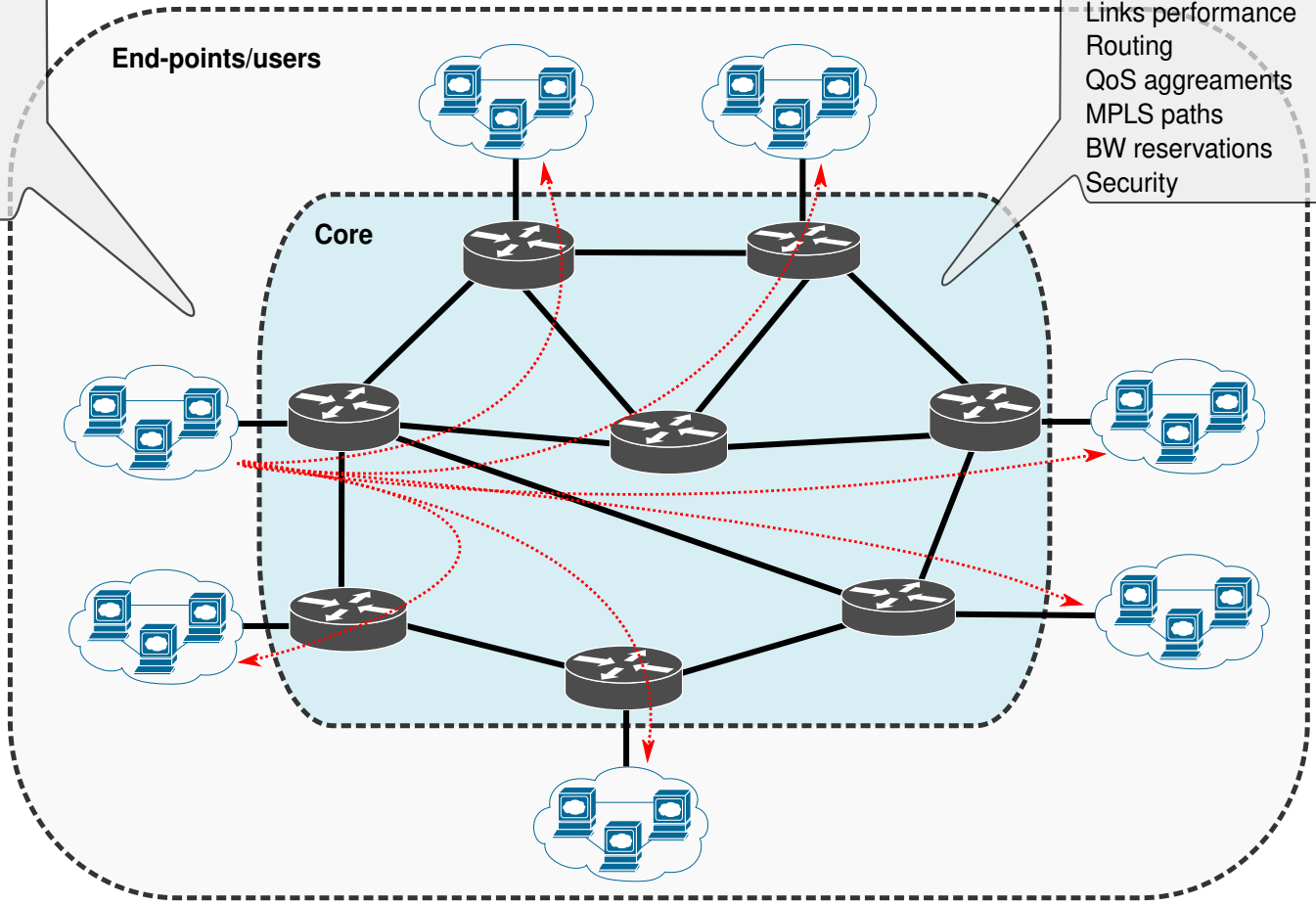
Core configurations
- Node awareness
- Service awareness

Nodes performance
Links performance
Routing
QoS aggreements
MPLS paths
BW reservations
Security

Core and End-to-End Monitoring

End-to-end measurements
- delay
- jitter
- throughput
- losses
- BW reservations
- reserved paths validation

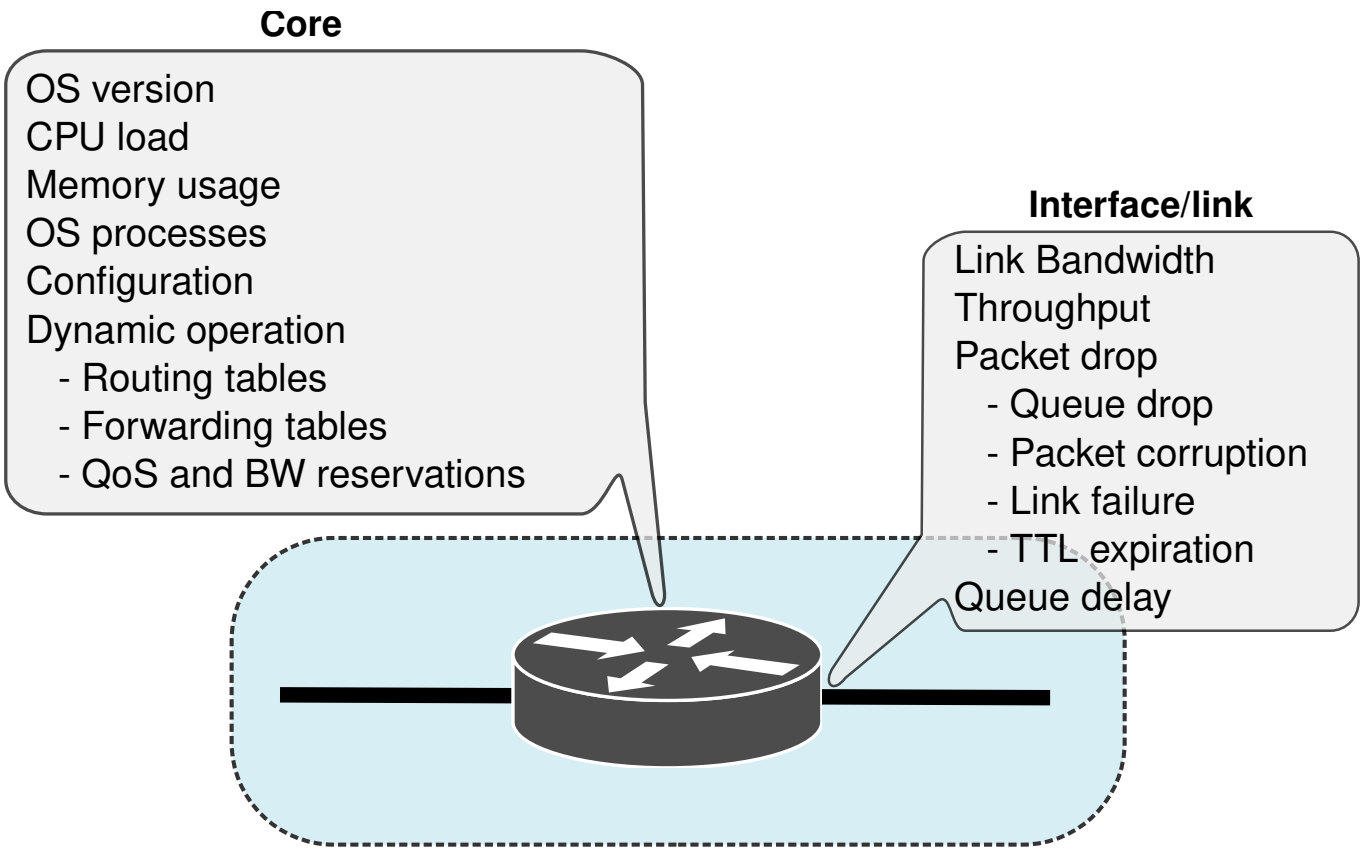
Demands per destination
- global
- per service/app
- per QoS usage



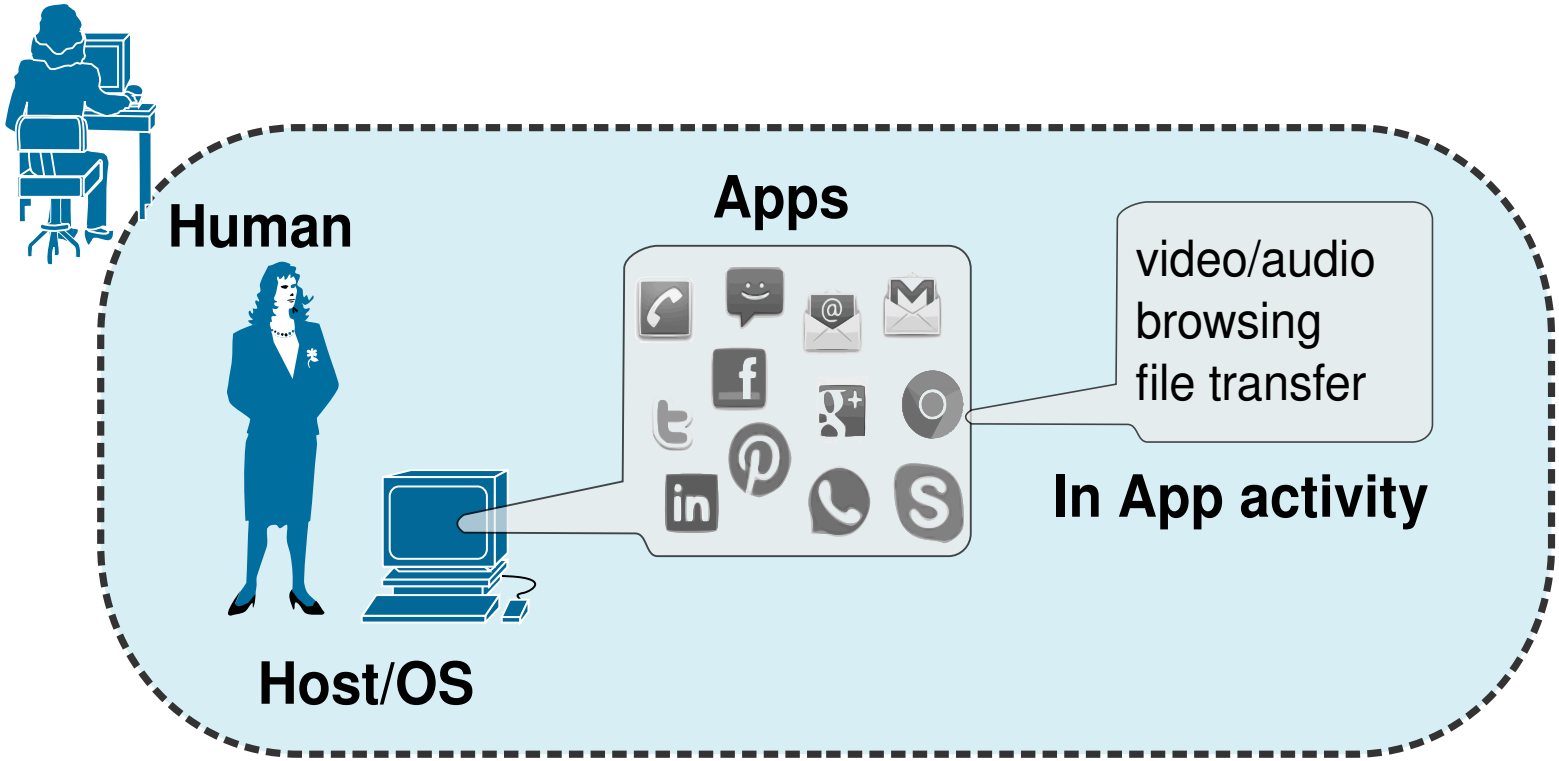
Core configurations
- Node awareness
- Service awareness

Nodes performance
Links performance
Routing
QoS aggreements
MPLS paths
BW reservations
Security

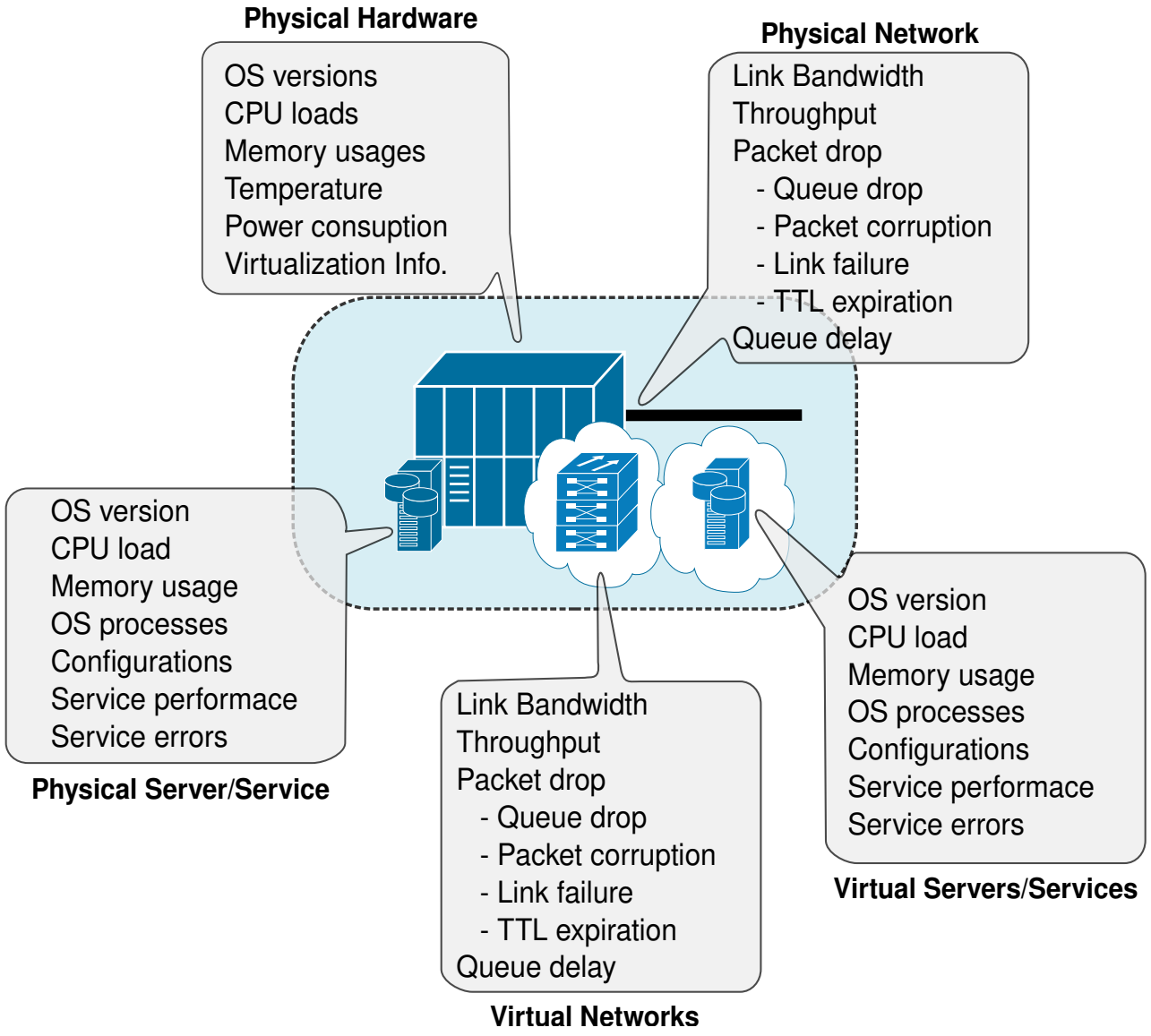
Node Monitoring



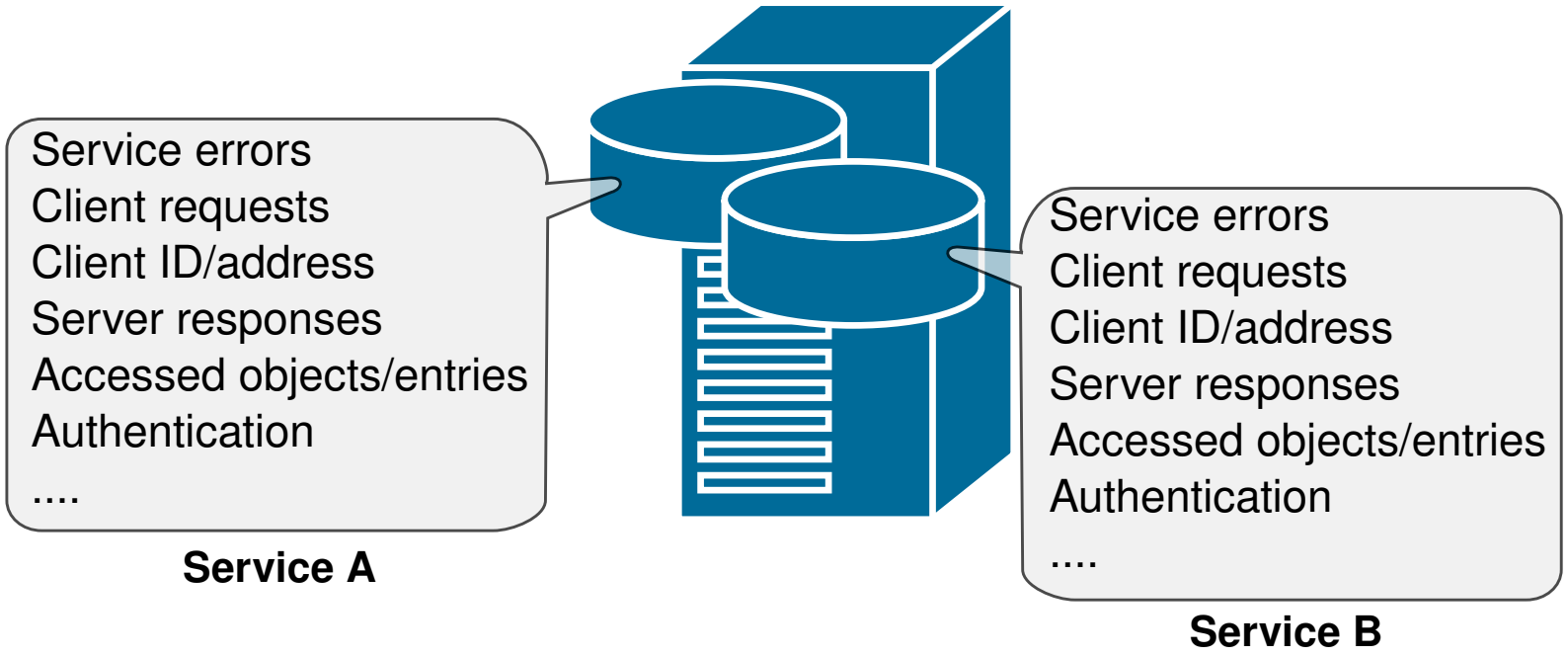
End-User/Host/App Monitoring



Server/Service/Cloud Monitoring



Per-Service Detailed Monitoring

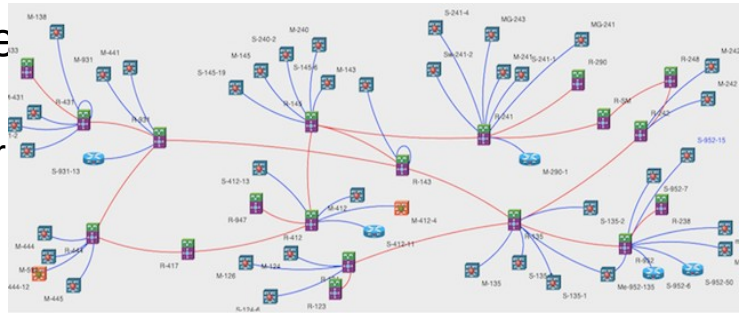


Data Sources

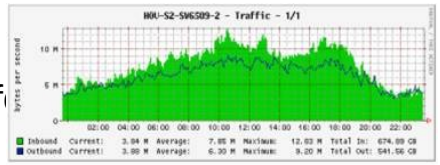
- SNMP
  - Used to acquire knowledge about current states of nodes/links/servers.
  - Local information. May be used to extrapolate to global information.
  - (Often) Requires the usage of vendor specific MIBs.
- Flow exporting
  - Used to characterize users/services in terms of amount of traffic and traffic destinations.
  - Medium and large time-scale information.
  - Protocols: Cisco NetFlow, IPFIX – Standard, Juniper jFlow, and sFlow
- Packet Captures / RAW statistics / DPI vs. SPI
  - Used to characterize users/services in small time-scales.
  - Requires distributed dedicated probes.
- Access Server/Device logs and/or CLI access.
  - Used to acquire knowledge about past and current state.
- Active measurements
  - Introduces entropy on network and requires (for many measurements) precise clock synchronization
  - E.g., one-way delay/jitter, round-trip delay/jitter.

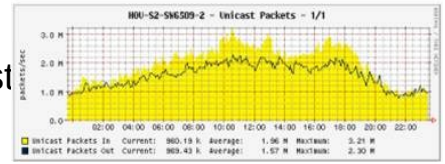
SNMP

- Used for acquiring the status and usage of node
  links and services over time.
  - Requires periodic pulling to obtain information over
- Used for obtain:
  - Network elements and interconnections,
  - Network deployed services.



- Used for estimating, characterizing, and predict:
  - Data flow performance.
    - Packet losses and (by indirect inference) delay/jitter at nodes.
    - Allows to obtain information about current and future service perf

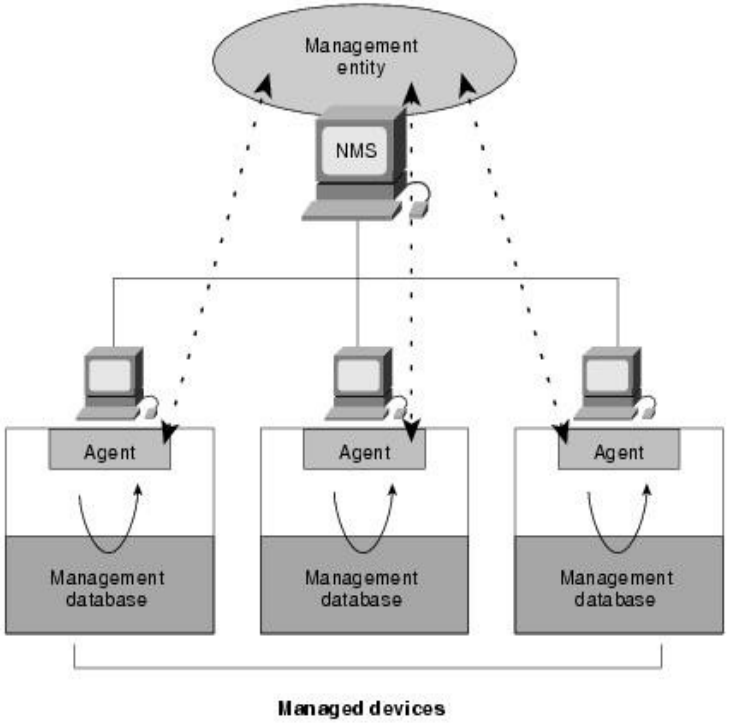




  - Nodes performance,
    - Memory/CPU usage, number of processes, etc...
    - Allows to detect points of failure, service degradation nodes, unst
  - Network link usage,
    - Ingress/egress bytes and packet counts.
    - Allows to perform optimizations in terms of routing (load balancing), link upgrade, and introduction of redundancy.
  - Data/flow routing,
    - At Layer 2, Layer 3 and MPLS levels.
    - Allows to understand how data flows and how may react to disruptive events.

SNMP Basic Components

- An SNMP-managed network consists of three key components:
- Managed devices
  - Network node that contains an SNMP agent.
  - Collect and store management information and make this information available using SNMP.
  - Can be routers and access servers, switches and bridges, hubs, computer hosts, or printers.
- Agents
  - Network-management software module that resides in a managed device.
- Network-management systems (NMSs)
  - Executes applications that monitor and control managed devices.
  - Provide the bulk of the processing and memory resources required for network management.
  - One or more NMSs must exist on any managed network.

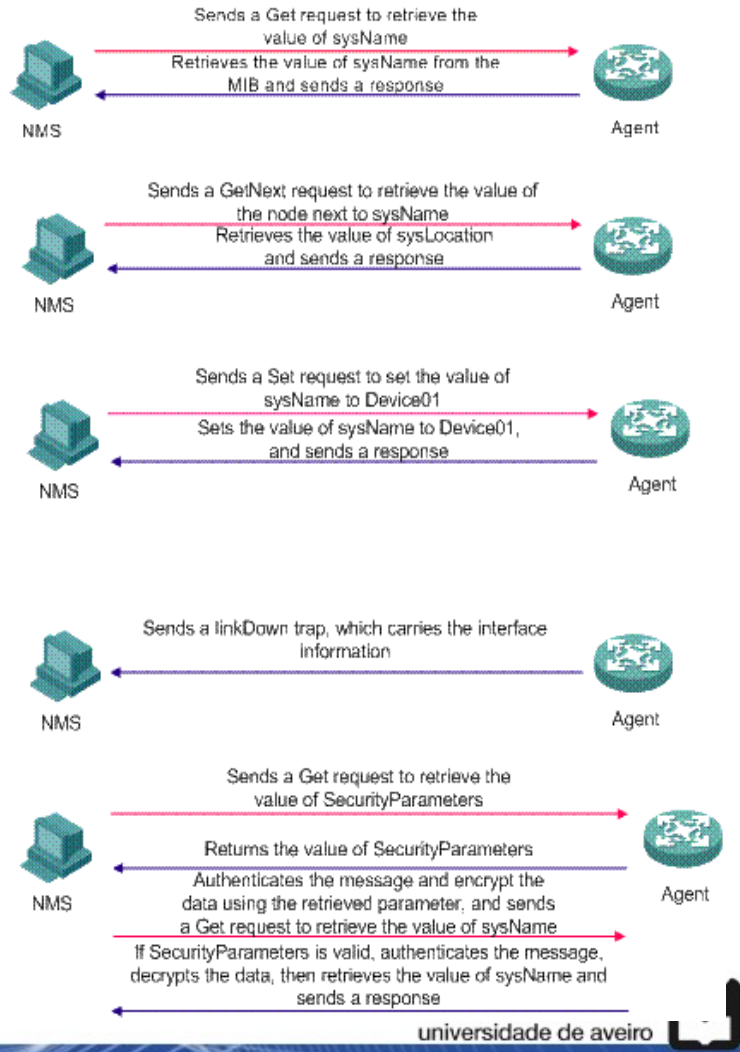


SNMP Versions

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithm.
v3	authPriv	MD5 or SHA	DES or AES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit or CFB128-AES-128 encryption in addition to authentication based on the CBC-DES (DES-56) standard.

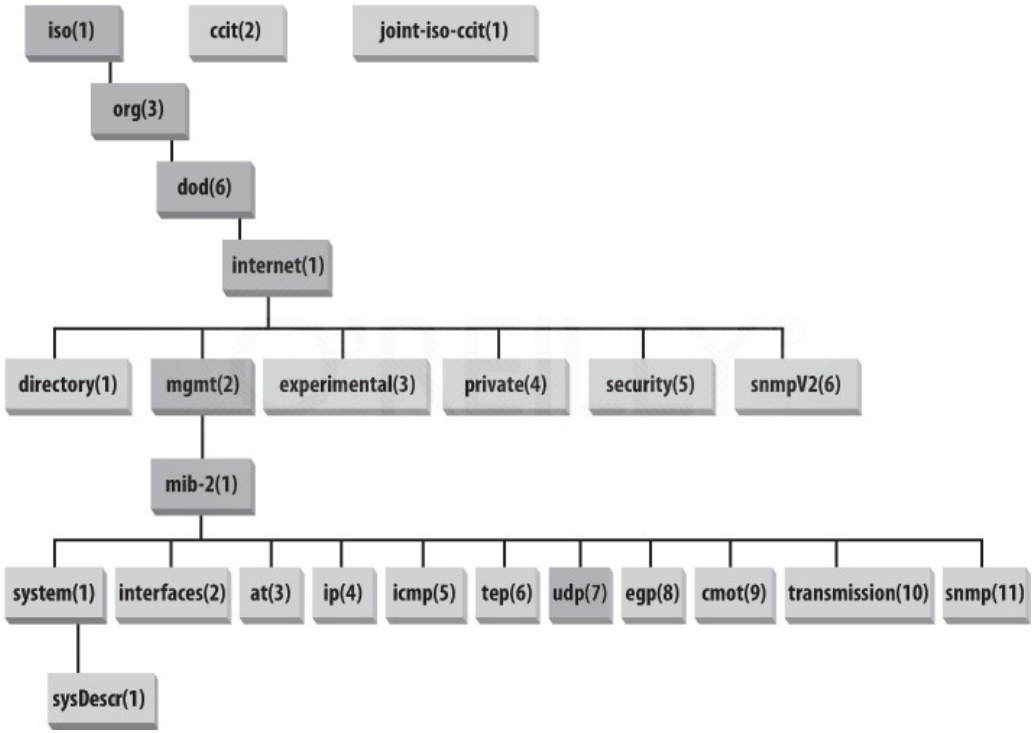
SNMP Operations

- SNMP provides the following five basic operations:
  - Get operation
    - Request sent by the NMS to the agent to retrieve one or more values from the agent.
  - GetNext operation
    - Request sent by the NMS to retrieve the value of the next OID in the tree.
  - Set operation
    - Request sent by the NMS to the agent to set one or more values of the agent.
  - Response operation
    - Response sent by the agent to the NMS.
  - Trap operation
    - Unsolicited response sent by the agent to notify the NMS of the events occurred.
- In SNMPv3 get operations are performed using authentication and encryption.



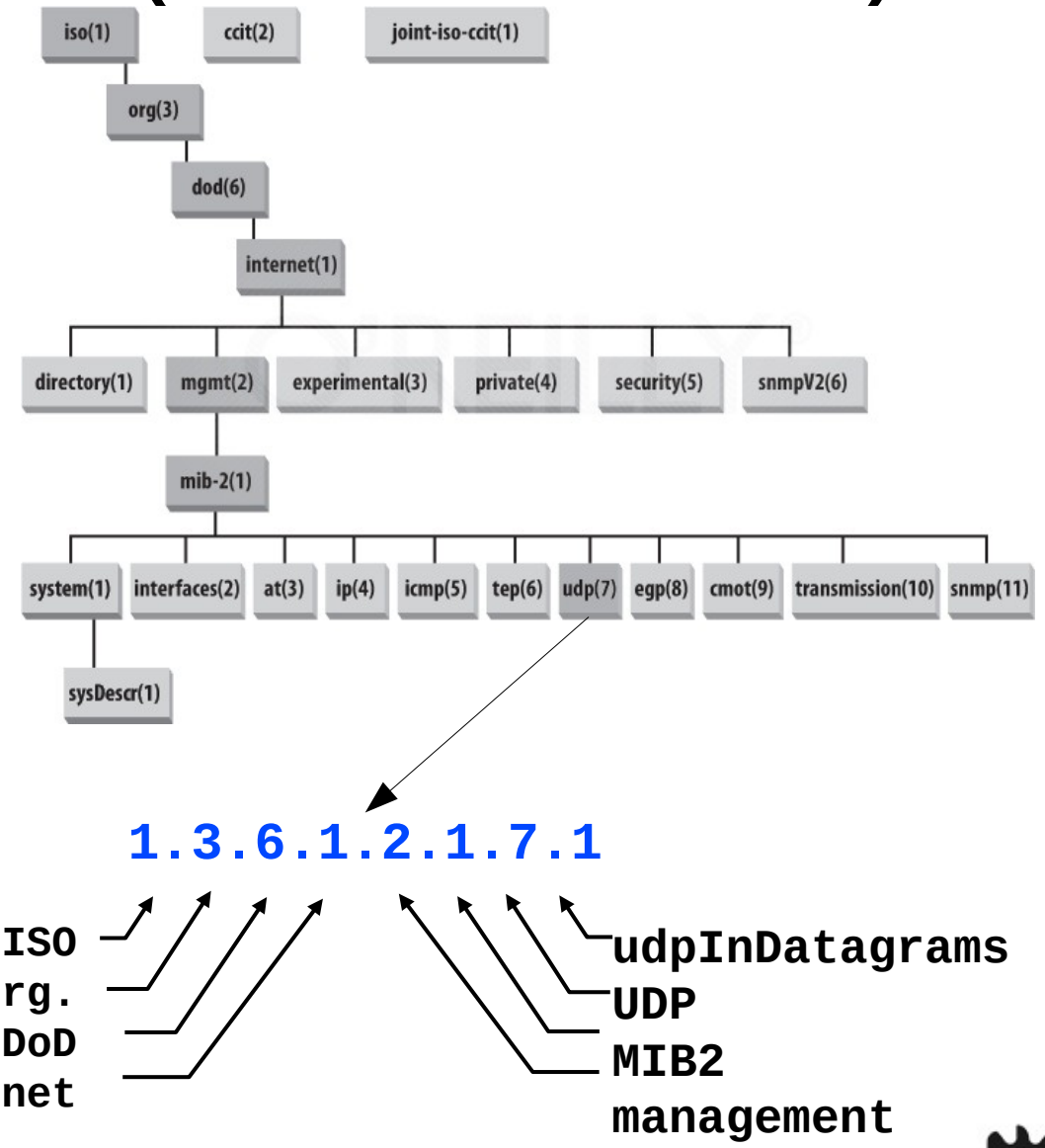
MIB Modules and Object Identifiers

- An SNMP MIB module is a specification of management information on a device
- The SMI represents the MIB database structure in a tree form with conceptual tables, where each managed resource is represented by an object
- Object Identifiers (OIDs) uniquely identify or name MIB variables in the tree
  - Ordered sequence of nonnegative integers written left to right, containing at least two elements
  - For easier human interaction, string-valued names also identify the OIDs
    - MIB-II (object ID 1.3.6.1.2.1)
    - Cisco private MIB (object ID 1.3.6.1.4.1.9)
- The MIB tree is extensible with new standard MIB modules or by experimental and private branches
  - Vendors can define their own private branches to include instances of their own products



SNMP Names (numbers/OID)

- To nominate all possible objects (protocols, data, etc.) it is used an ISO Object Identifier (OID) tree:
  - Hierarchic nomenclature of objects
  - Each leaf of the tree has a name and number



SNMP MIBs

- Management Information Base (MIB): set of managed objects, used to define information from equipments, and created by the manufacturer
- Example: UDP module

Object ID	Name	Type	Comments
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	Number of UDP datagrams delivered to users.
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	Number of received UDP datagrams for which there was no application at the destination port.
1.3.6.1.2.1.7.3	UDPInErrors	Counter32	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	The total number of UDP datagrams sent from this entity.

Relevant MIBs

- Interface characteristics, configurations, status, ans stats:
  - IF-MIB and IP-MIB.
  - Cisco extra information: CISCO-QUEUE-MIB, CISCO-IF-EXTENSION-MIB
- Nodes management information (description, general information, CPU/memory status, etc...):
  - SNMPv2-SMI and ENTITY-MIB.
  - Vendor specific: CISCO-SMI, JUNIPER-SMI, etc...
  - Cisco extra: CISCO-PROCESS-MIB, CISCO-FLASH-MIB, CISCO-ENVMON-MIB, CISCO-IMAGE-MIB, etc...
- Node routing and traffic-engineering:
  - IP-MIB, IP-FORWARD-MIB
    - Cisco extra information: CISCO-CEF-MIB, CISCO-PIM-MIB
  - MPLS-TE-MIB, MPLS-LSR-MIB, MPLS-VPN-MIB
- Node services:
  - Vendor specific: CISCO-AAA-SESSION-MIB, CISCO-SIP-UA-MIB, etc...
- Node monitoring mechanisms:
  - RMON-MIB, RMON2-MIB, CISCO-SYSLOG-MIB, CISCO-RTTMON-MIB, CISCO-NETFLOW-MIB, CISCO-IPSEC-FLOW-MONITOR-MIB, etc...

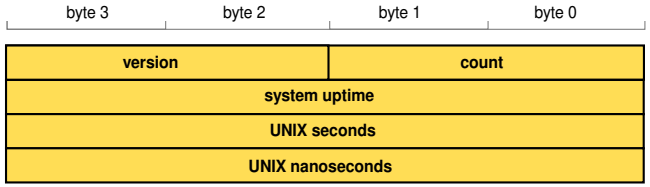
NetFlow

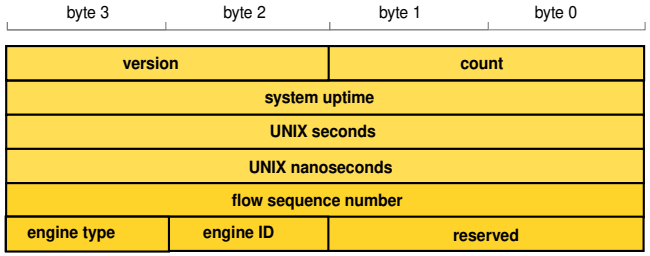
- Cisco NetFlow services provide network administrators IP flow information from their data networks.
  - Network elements (routers and switches) gather flow data and export it to collectors.
  - Captures data from ingress (incoming) and/or egress (outgoing) packets.
  - Collects statistics for IP-to-IP and IP-to-MPLS packets.
- A flow is defined as a unidirectional sequence of packets with some common properties that pass through a network device.
  - A flow is identified as the combination of the following key fields:
    - Source IP address, Destination IP address, Source port number, Destination port number, Layer 3 protocol type, Type of service (ToS), and Input logical interface.
- These collected flows are exported to an external device, the NetFlow collector.
- Network flows are highly granular
  - For example, flow records include details such as IP addresses, packet and byte counts, timestamps, Type of Service (ToS), application ports, input and output interfaces, autonomous system numbers, etc.
- NetFlow has three major versions: v1, v5 and v9.
  - v1 is only recommended for legacy devices without support to v5 or v9.
  - V1 and v5, do not support IPv6 flows.

NetFlow versions 1 and 5

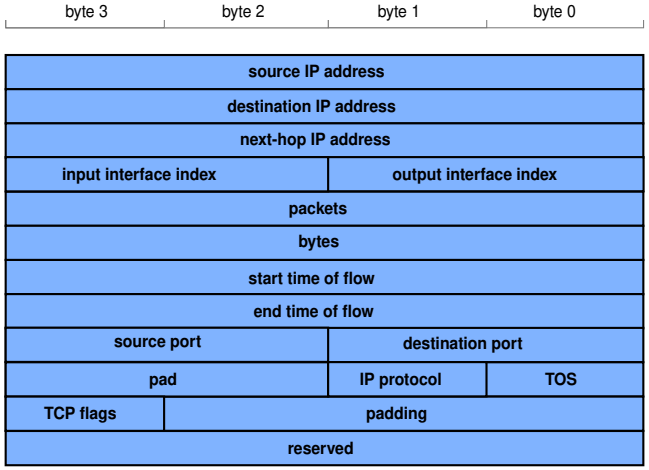
- NetFlow v1/v5 packets are UDP/IP packets with a NetFlow header and one or more NetFlow data Records

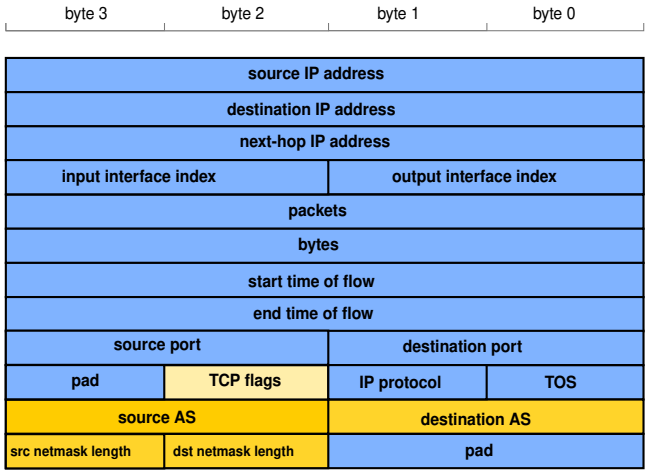
Header format





Record format



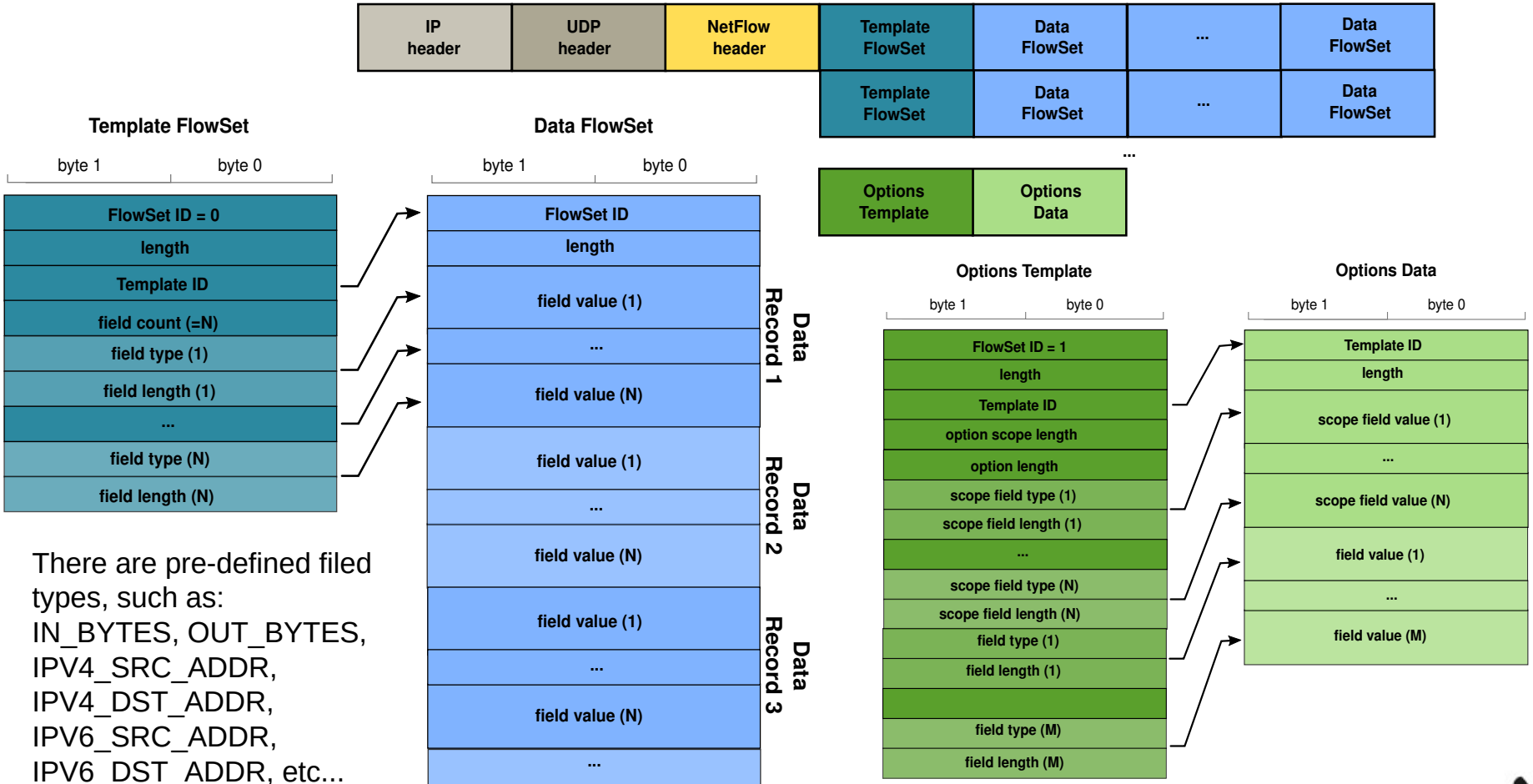


Version 1

Version 5

NetFlow version 9

- NetFlow v9 packets are UDP/IP packets with a NetFlow header, one or more Template FlowSets (may be suppressed, if sent previously), one or more Data FlowSets, and, optionally, an Options Template and Data Record.



There are pre-defined filed types, such as:
IN_BYTES, OUT_BYTES,
IPV4_SRC_ADDR,
IPV4_DST_ADDR,
IPV6_SRC_ADDR,
IPV6_DST_ADDR, etc...

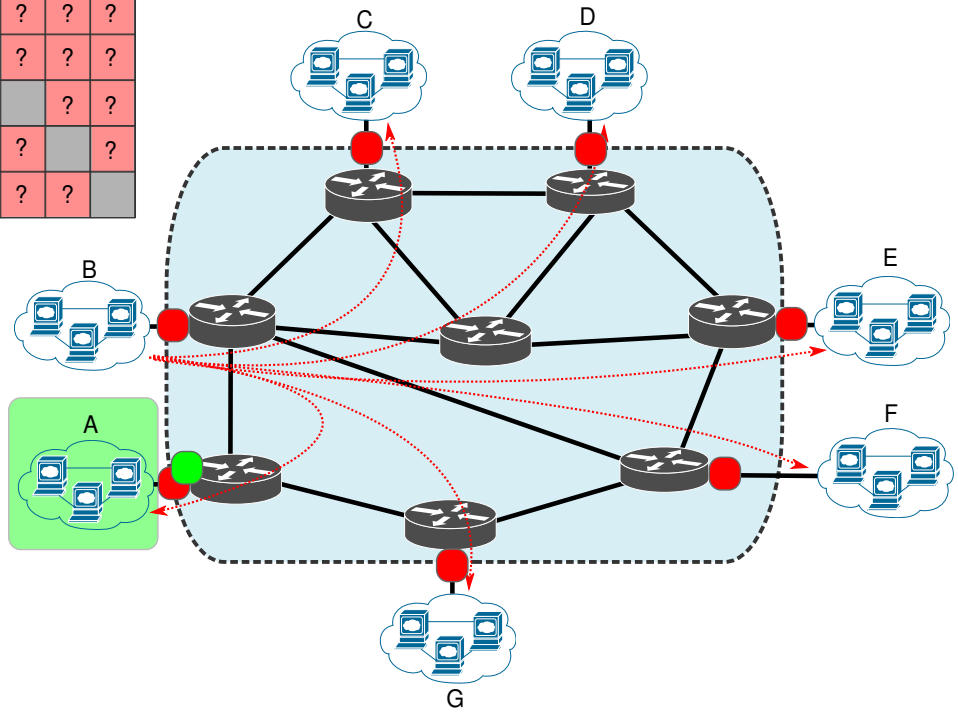
NetFlow Usage

- Used to characterize users/services in terms of amount of traffic.
  - Users/Groups (overall or per-app) → Applied in (V)LAN interfaces.
  - Services → Applied to data-center interfaces
- Used to characterize traffic destinations (to egress points) from a specific ingress point in a network: traffic matrices.
  - Ingress/Egress points may be:
    - Network access links (distribution layer L3SW, Internet access routers, user VPN server links),
    - Network core border links (core border routers),
    - BGP peering links (AS Border routers).
- Used to characterize “in network” routing.
  - Complex to implement and process.

NetFlow Deployment

- Interfaces to monitor depend on objective:
  - Traffic matrix inference – all core border interfaces.
  - User/group flow generation inference - access interface from user/group.
- Egress vs. Ingress monitoring:
  - Traffic matrix inference – ingress OR egress.
  - User/group flow generation inference – both directions.

	A	B	C	D	E	F	G
A		?	?	?	?	?	?
B	?		?	?	?	?	?
C	?	?		?	?	?	?
D	?	?	?		?	?	?
E	?	?	?	?		?	?
F	?	?	?	?	?		?
G	?	?	?	?	?	?	

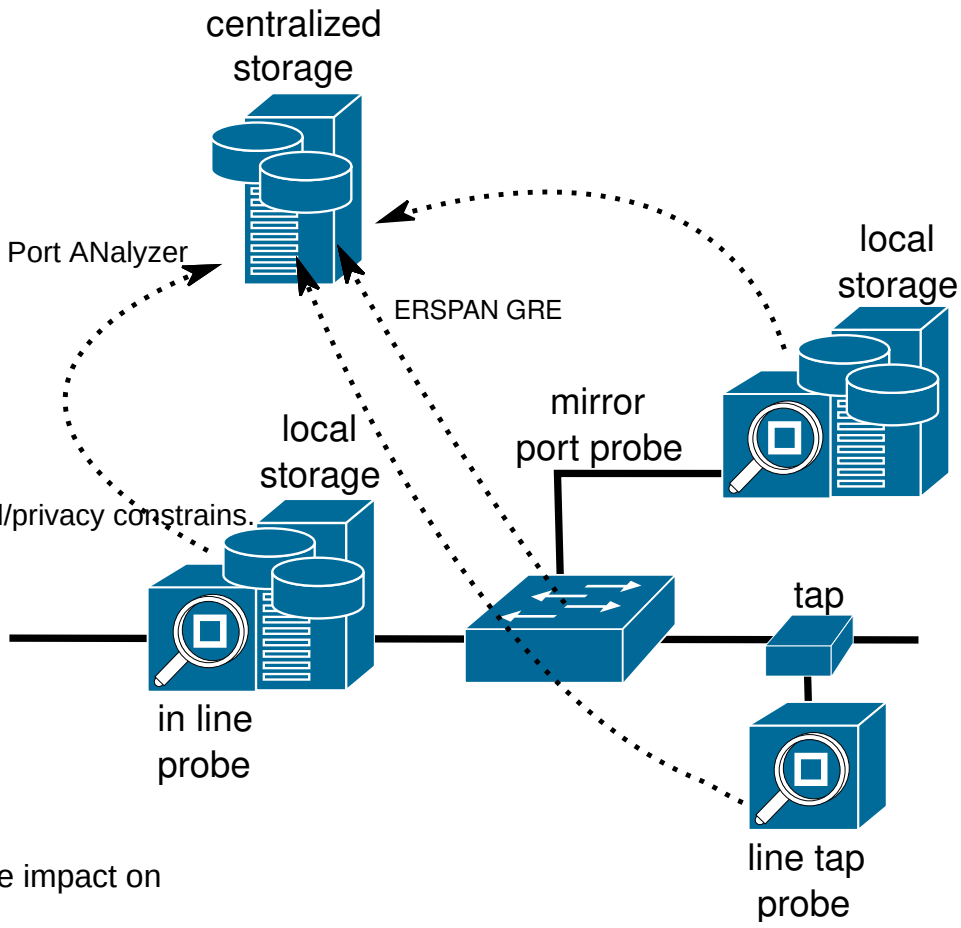


IPFIX (v10) and Flexible NetFlow

- IPFIX is very similar to NetFlow v9
  - Uses version 10 in a similar header.
  - Also has Templates and Data Records.
  - Also has Options Templates and Options Data Records.
- IPFIX made provisions for NetFlow v9 and added support for it.
  - IPFIX lists an overview of the “Information Element identifiers” that are compatible with the “field types” used by NetFlow v9.
- IPFIX has more filed types than the ones defined for NetFlow v9.
  - Also allows a vendor ID to be specified which a vendor can use to export proprietary/generic information.
- IPFIX allows for variable length fields.
  - Useful to export variable size strings (e.g., URLs).
- NetFlow v9 extension “Flexible NetFlow” aims to be equally flexible as IPFIX.

Network Passive Probing

- User for:
  - Specific and detailed data inference,
  - Infer small and medium timescale dynamics.
- Probe types
  - Switch mirror port,
  - In-line,
  - Network tap.
  - ERSPAN GRE tunnel from switch.
    - ERSPAN: Encapsulated Remote Switched Port ANalyzer
- Filtering/sampled by
  - User/terminal address/VLAN/access port,
  - Group address/VLAN/access port,
  - Protocols (UDP/TCP),
  - Upper layer protocols,
    - Hard to identify due to encryption and legal/privacy constrains.
  - UDP/TCP port number/range.
- Data processing
  - Packet/byte count,
  - Flow count,
  - IP addresses and port distribution,
  - App/service statistics and distribution.
- Local vs. Centralized storage and processing.
  - Data upload to centralized point should not have impact on measurements.
  - Local storage/processing requires probes with more resources.



Log Management Systems (LMS)

- Software system that aggregates and stores log files from multiple network sources and systems.
- Allows organizations to centralize all of their log data from multiple systems.
- Allows Logs to be viewed and correlated.
- Main purposes:
  - Detect and respond to Indicators of Compromise (IoC);
  - Conduct forensic data analysis;
  - Perform investigations into network events and possible attacks.

Security Information and Events Management (SIEM)

- Incorporates three types of security tools into a single application:
  - Security Event Management (SEM)
    - Very similar to LMS.
    - Aggregates log files from multiple systems, but they are more geared towards the needs of IT security analysts instead of system administrators.
  - Security Information Management (SIM)
    - Software tools used to identify, collect, and analyze data from event logs.
    - Include automated features and alerts that can be triggered when predetermined conditions are satisfied that might indicate that the network is compromised.
    - Help security analysts automate the incident response process and generate more precise reports on the organization's security position/past.
  - Security Event Correlation (SEC)
    - Software used to process ans search massive quantities of event logs and discover correlations and connections between events that could indicate a security issue.

LMS vs. SIEM

- LMS tools are more focused on:
  - Log Data Collection, efficient Retention of Data, log indexing and search functions, ans reporting.
- SIEM tools are more focused on:
  - Threat detection alerts, event correlation, and dash-boarding (real-time monitoring with custom events visibility).
- Evolution of traditional LMS, designed mainly for system administration support, made them functionally much closer to SIEM tools developed from scratch as a security tool.

SIEM Events (examples)

- Brute force detection
  - Excessive 404 errors (HTTP server Log) from a non-authenticated client (DB Log).
  - Excessive login failures (services or DB Logs) at one or multiple services.
    - From a specific IP address (or set of IP addresses).
    - From “strange” geographic regions or AS.
  - Non-matching credentials
    - From internal machines with non-matching user credentials (RADIUS/LDAP Logs).
- Impossible travel
  - Multiple logins from same user from different devices/locations.
  - Consecutive logins from same user from distant geographic regions within a small time window. VPN usage may trigger such an alarm.
- Anomalous data transference
  - Analyzing by individual source (IP or device group) and/or destination and/or by used protocol/port.
  - Excessive/Different data transference not compatible with past observations
    - Protocols and ports usage;
      - Usually firewall rules solve this!
    - Download/upload amounts, number of connections, ratio upload/download, ratio DNS/non-DNS, etc…;
    - Never contacted devices: external servers (unknown IP/ASN or country) or internal devices,;
    - Absolute time of day/week/month.
    - Relative time activity: mean or standard deviation of intervals between activity/flows/requests/etc...
  - Should be used to detect exfiltration (or propagation inside the network) and illicit C&C and data channels.
- DDoS attack
  - Excessive connection attempts from “never seen” devices/addresses/regions.
    - Ideal detection in the early phase of the attack.
  - Non-excessive attempts, but non-conformal behavior (time behavior, sequence of requests,etc...)
    - More difficult to define.
- Files/Configurations integrity fails
  - Specific device/service configuration file checksum failure, non justifiable by observed actions.
  - Generic file checksum failure, non justifiable by observed actions.
- Etc… ?

Security Operations Center (SOC)

- Competences of a SOC in an organization:
  - Prevention and detection of attacks
    - Monitor network and services (with SIEM)
    - Detect vulnerabilities (with vulnerability scanning tools)
    - Detect malicious activities (with SIEM)
    - Detect anomalous behaviors (with SIEM)
      - may not be malicious!
  - Investigation
    - Analyze the suspicious activity to determine/characterize the threat
    - Evaluate how deep the threat has penetrated the network/systems
  - Response
    - Deploy counter measures based on known playbooks
    - Deploy emergency measures when threat do not match a known response playbook
  - Forensics
    - Done after an attack
    - Gather evidences for judicial purposes
    - Gather additional data to improve future prevention/detection/response
- Nowadays commonly operated independently of the Network Operation Center (NOC).
- Should be integrated with NOC.
  - For network/services segregation and resilience, data acquisition and threat mitigation.

Security Metrics/KPI

- Access management
  - How many users have administrative access, and how often is used.
  - Shared passwords between staff.
- Preparedness
  - Percentage of devices fully patched and up to date.
- Days to patch
  - Average time between patch availability and deployment.
- Unidentified devices
  - Illicitly deployed devices.
  - BYoD policy, legacy devices, unlisted devices, IoT devices, etc...
- Security devices average/maximum load per time period.
- Intrusion attempts
  - Amount of detected and undetected attempts (in real time or after off-line auditing).
- Cost per incident
  - Includes staff overtime, external support, investigation costs, employee productivity loss, loss of communication, service failure, etc…
- Mean Time Between Failures (MTBF)
  - Average time between failures (hardware and/or software).
  - General or per device/service.
- Mean Time to Recovery (MTTR)
  - Average time between failure and recovery (hardware and/or software).
- Mean Time to Detect (MTTD)
  - Average time between intrusion and detection.
- Mean Time to Acknowledge (MTTA)
  - Average time between detection and start of countermeasures deployment.
- Mean Time to Contain (MTTC)
  - Average time between start of countermeasures deployment and complete mitigation.
- Mean Time to Resolve (MTTR)
  - MTTA+MTTR