

IT Infrastructure Architecture

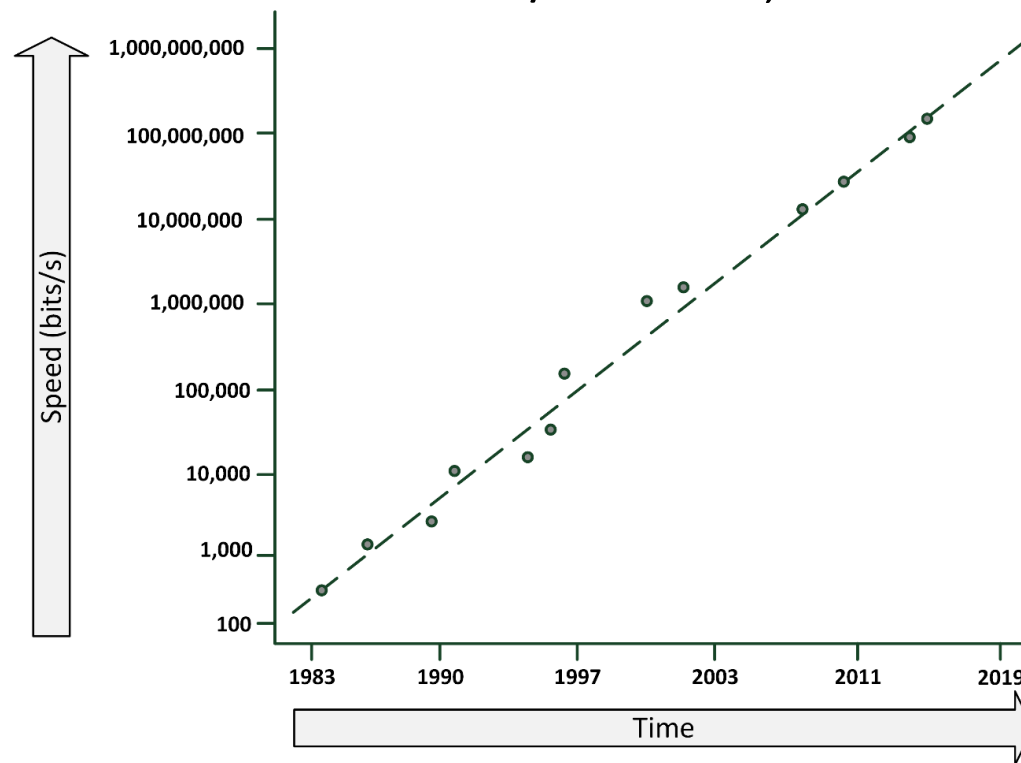
Infrastructure Building Blocks
and Concepts

Networking

Network performance

Nielsen's law

- Network connection speeds for high-end home users increase 50% per year, they double every 21 months
- Bandwidths should be 15 Gbit/s in 2025, for about \$50 per month



Please note that the vertical scale is logarithmic instead of linear

Throughput and bandwidth

- Throughput is the amount of data that is transferred through the network during a specific time interval
- Throughput is limited by the available bandwidth
- When an application requires more throughput than a network connection can deliver:
 - Queues in the network components temporarily buffer data
 - Buffered data is sent as soon as the network connection is free again
 - When more data arrives than the queues can store in the buffer, packet loss occurs

Latency

- Latency is defined as the time from the start of packet transmission to the start of packet reception
- Latency is dependent on:
 - The physical distance a packet has to travel
 - The number of switches and routers the packet has to pass
- Rules of thumb:
 - 6 ms latency per 100 km
 - WANs: Each switch in the path adds 10 ms to the one-way delay
 - LANs: add 1 ms for each switch

Latency

- One-way latency: the time from the source sending a packet to the destination receiving it
- Round-trip latency: the one-way latency from source to destination plus the one-way latency from the destination back to the source
- “ping” can be used to measure round-trip latency

Quality of Service (QoS)

- Quality of service (QoS) is the ability to provide different data flow priority to different applications, users, or types of data
- QoS allows better service to certain important data flows compared to less important data flows
- QoS is mainly used for real-time applications like video and audio streams and VoIP telephony

Quality of Service (QoS)

- Four basic ways to implement QoS:
 - Congestion management
 - Defines what must be done if the amount of data to be sent exceeds the bandwidth of the network link
 - Packets can either be dropped or queued
 - Queue management
 - When queues are full, packets will be dropped
 - Queue management defines criteria for dropping packets that are of lower priority before dropping higher priority packets

Quality of Service (QoS)

– Link efficiency

- Ensures the link is used in an optimized way
- For instance by fragmenting large packets with a low QoS, allowing packets with a high QoS to be sent between the fragments of low QoS packets

– Traffic shaping

- Limiting the full bandwidth of streams with a low QoS to benefit streams with a high QoS
- High QoS streams have a reserved amount of bandwidth

WAN link compression

- Data compression reduces the size of data before it is transmitted over a WAN connection
- WAN acceleration appliances:
 - Provide compression
 - Perform some caching of regularly used data at remote sites

Network security

Firewalls

- Firewalls separate two or more LAN or WAN segments for security reasons
- Firewalls block all unpermitted network traffic between network segments
- Permitted traffic must be explicitly enabled by configuring the firewall to allow it
- Firewalls can be implemented:
 - In hardware appliances
 - As an application on physical servers
 - In virtual machines
- Host based firewalls
 - Protect a server or end user computer against network based attacks
 - Part of the operating system

Firewalls

- Firewalls use one or more of the following methods to control traffic:
 - Packet filtering
 - Data packets are analyzed using preconfigured filters
 - This functionality is almost always available on routers and most operating systems
 - Proxy (also known as application layer firewalls)
 - A proxy terminates the session on the application level on behalf of the server (proxy) or the client (reverse proxy) and creates a new session to the client or server
 - Stateful inspection
 - Inspects the placement of each individual packet within a packet stream
 - Maintains records of all connections passing through the firewall and determines whether a packet is the start of a new connection, part of an existing connection, or is an invalid packet

IDS/IPS

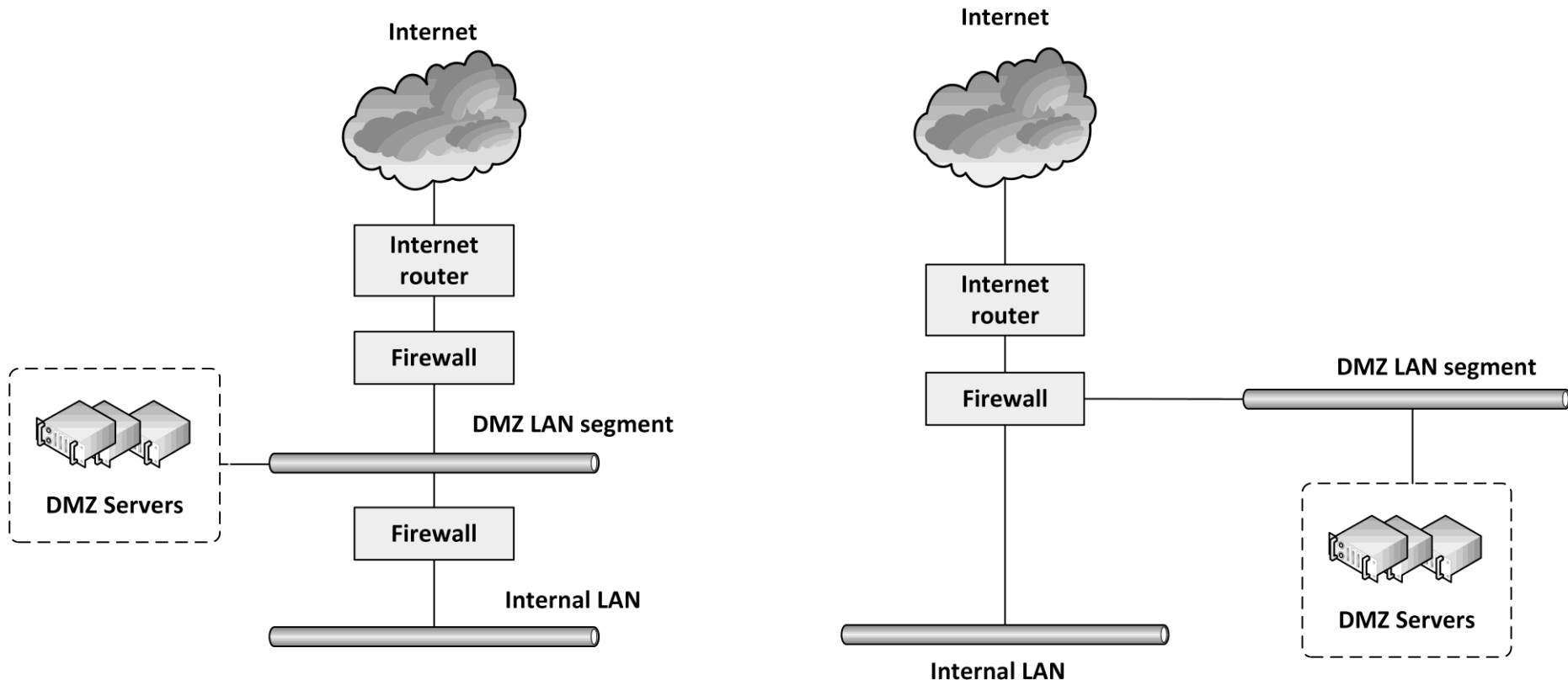
- An Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) detects and – if possible – prevents activities that compromise system security, or are a hacking attempt
- An IDS/IPS monitors for suspicious activity and alerts the systems manager when these activities are detected
- An IPS can stop attacks by changing firewall rules on the fly

IDS/IPS

- Two types of IDS/IPS systems:
 - A Network-based IDS (NIDS) is placed at a strategic point in the network
 - Monitors traffic to and from all devices on that network
 - The NIDS is not part of the network flow, but just “looks at it”, to avoid detection of the NIDS by hackers
 - A Host-based IDS (HIDS) runs on individual servers or network devices
 - It monitors the network traffic of that device
 - It also monitors user behavior and the alteration of critical (system) files

DMZ

- DMZ is short for De-Militarized Zone, also known as screened subnet, or the Perimeter Network
- A DMZ is a network that serves as a buffer between a secure protected internal network and the insecure internet



RADIUS

- Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized user and authorization management for network devices
 - Routers
 - Modem servers
 - Switches
 - VPN routers
 - Wireless network access points
- RADIUS
 - Authenticates users or devices before granting them access to a network
 - Authorizes users or devices for certain network services

Network Access Control (NAC)

- Network Access Control (NAC) is used at the network end points, where end user devices (like laptops) can be connected to the network
- It allows predefined levels of network access based on:
 - A client's identity (is the laptop known to the organization?)
 - The groups to which a client belongs
 - The degree to which a client's device complies with the organization's governance policies (does it run the most recent virus scanner?)

Network Access Control (NAC)

- If a client device is not compliant, NAC provides a mechanism to automatically bring it into compliance
- For instance:
 - Installing the latest virus scanner updates while connected on an isolated LAN segment
 - After the update finishes, access is granted to the rest of the network