PA197 Secure Network Design
3. Security Architectures I

Eva Hladká, Luděk Matyska

Faculty of Informatics

March 7, 2016

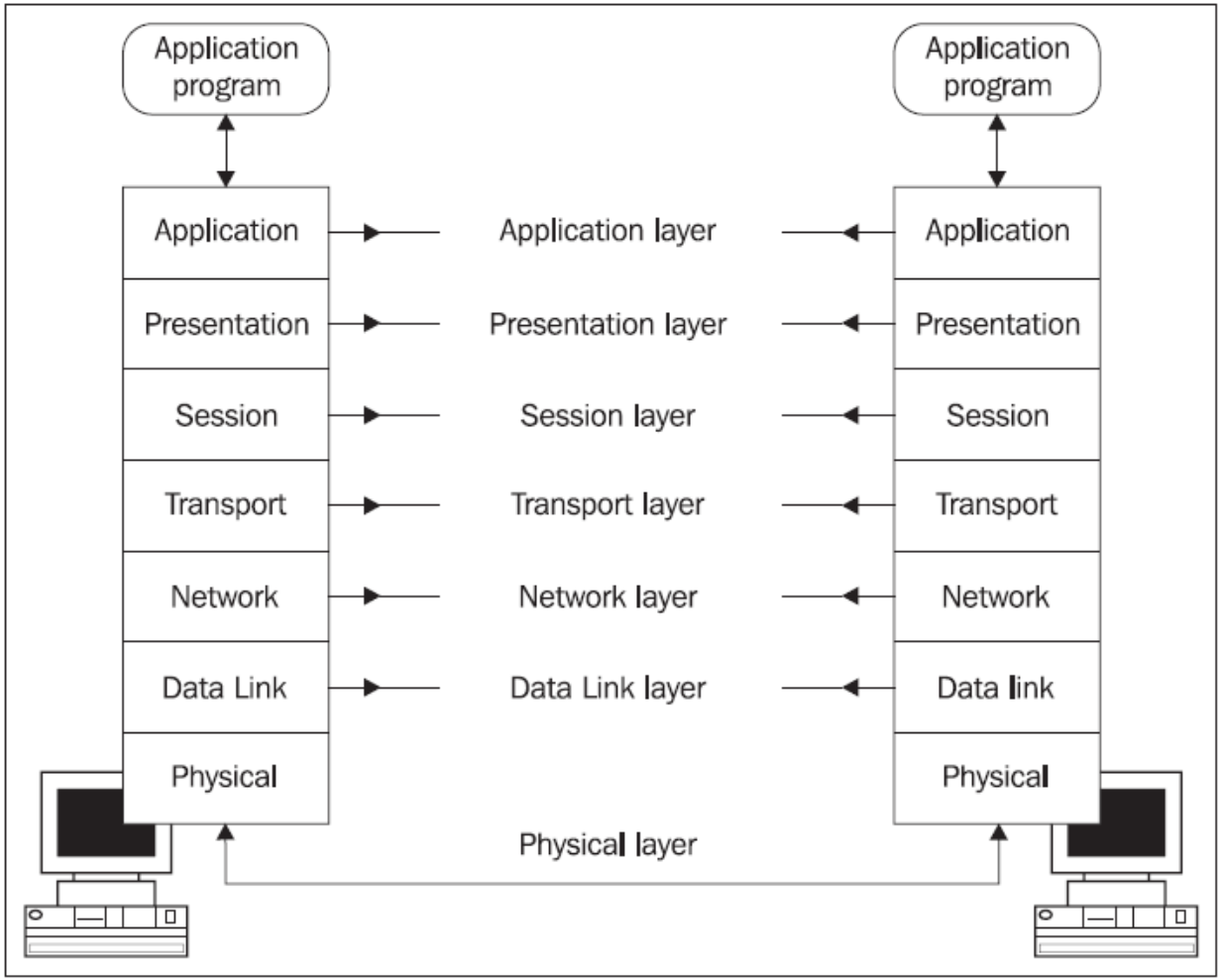
Content

Internet protocols

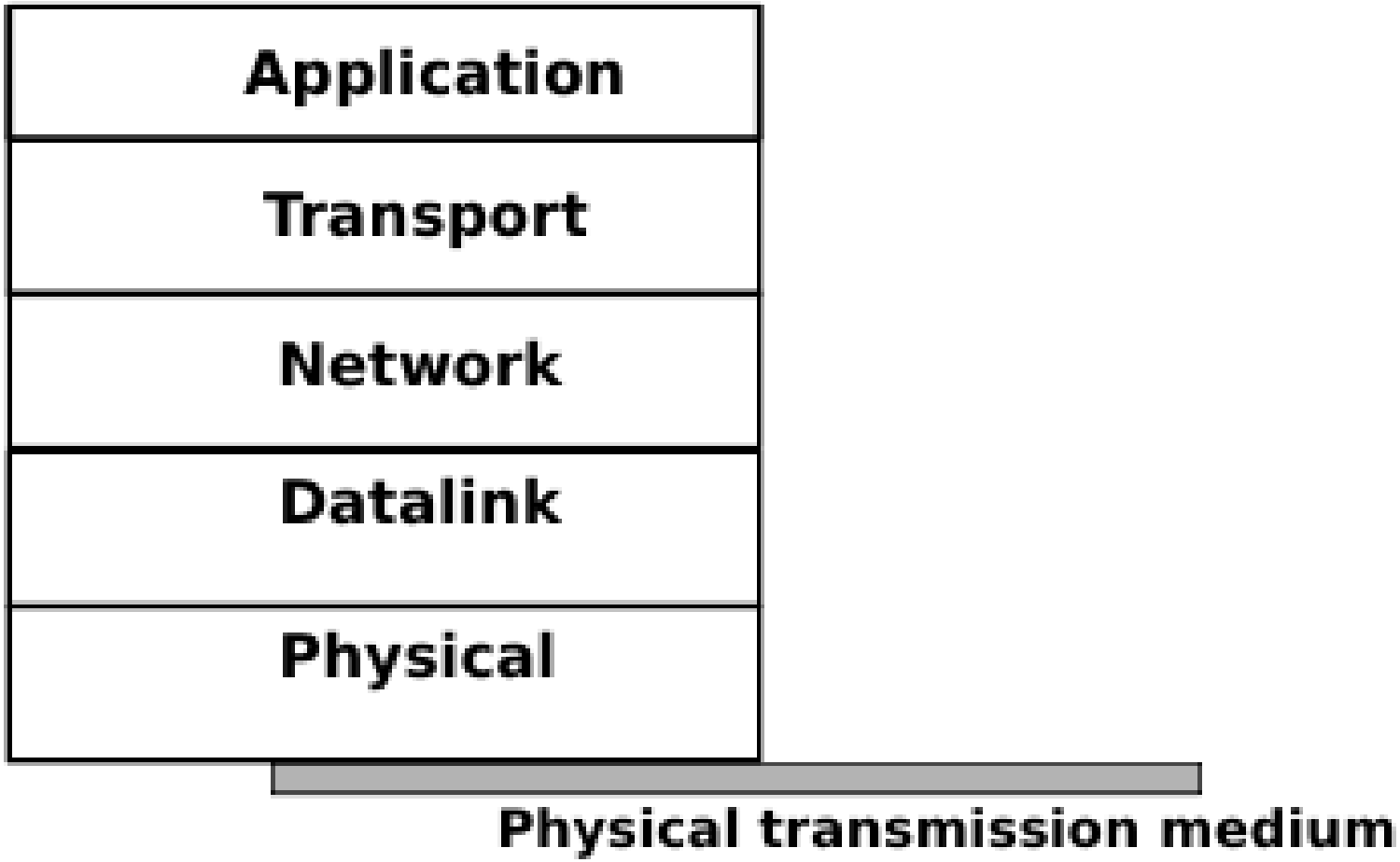
- Networks rely on protocols
  - a communication protocol is a set of rules that define how data are exchanged between computers
- A protocol defines
  - syntax
  - semantics
  - synchronization

  independent on the implementation
- Protocol layering
  - basic design principle
  - allows decomposition

OSI Reference Model



TCP Reference Model



Transport Layer

- Communication between application programs
  - end-to-end
  - whole messages
    - split into packets at Internet layer
- Transmission Control Protocol (TCP)
  - reliable transport
  - flow/congestion control
- User Datagram Protocol (UDP
  - unreliable transport
  - connection-less

TCP—reliable protocol?

- Provides reliable transport
  - byte-oriented stream
  - guarantees ordering
  - guarantees integrity
- However, the guarantees not prone against active adversary
  - man-in-the-middle: easy to modify
    - source address
    - content
  - sequence prediction attack
    - injects counterfeit attacks

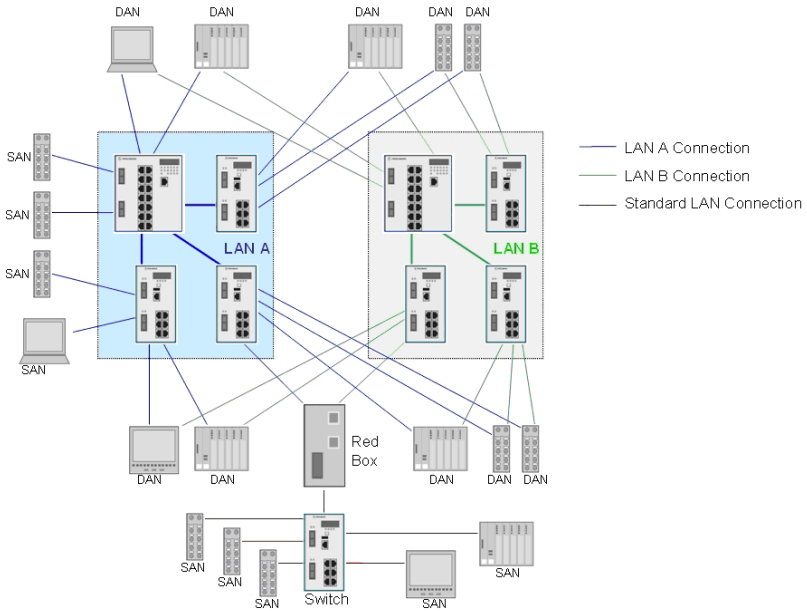
Redundancy principle

- Redundancy: and old engineering principle
  - do not create (remove) any single point of failure (SPOF)
  - failure in one component could not crash the system
- A design principle to prevent a failure of the whole system
- It comes with added cost and complexity
- Cost implications
  - more components than actually needed to perform an operation
  - cost limits the extent of redundancy
    - i.e. how many components could fail before the system goes down
- Complexity implications
  - adding components makes the system more complex
  - higher complexity increases the probability of a failure
    - RYF-principle (Robust Yet Fragile)
- Redundancy is not a backup

Redundancy in network design

- Needs to have multiple instance of everything that can possibly fail
  - links
  - ports
  - active elements

  Everything must be at least doubled (no SPOF)
- *The principle demonstration*



Availability

- Redundancy is a tool, availability is the goal
  - we would like to have always available systems
  - in practice, high availability is achievable
- Redundancy contributes to availability keeping the system up in presence of failures
- Reaction in case of failure:
  - failure detection
  - failing over
  - reconnection
- Network protocols have different parts implemented
  - routing used as the next example

Link protection

- A scheme to mitigate from network failure
  - link layer
  - end nodes of the link responsible for failover
- Basic principles
  - failure recognition
  - selection of redundant path
- Bi-directional Line Switched Ring (BLRS)
  - every link can carry payload and backup traffic at the same time
  - four fiber
    - two fibers for working
    - two fibers for protection/backup
  - two-fiber
    - work and backup shared
    - half the capacity for backup

Link protection–Ethernet

- Link aggregation
  - multiple links carry the traffics
    - failure of a single link reduces the overall throughput

  the redundancy principle in practice
- Initially static configuration
  - high probability of configuration error
  - not able to properly detect the failure
- Dynamic configuration
  - Link Aggregation Control Protocol (see next slides)

Path protection

- Protect from network failure in connection oriented networks
- Ring
- Optical Mesh
- MPLS (Multi Protocol Label Switching)
  - packet protection scheme
    - two link/node disjoint paths between ingress and outgress routers
    - outgress router compares packets
    - uses double the bandwidth
  - global path protection
    - primary and backup label switched path (LSP) are computed and setup
    - the backup may not fulfill the SLA
    - backup LSP does not carry traffic
    - fault indication signal inform ingress router to switch to backup LSP

Link aggregation

- Combining (aggregating) multiple network connections to
  - increase throughput
  - provide redundancy
- The lowest three layers
  - layer 1: IEEE 1901 (power line) or IEEE 802.11 (wireless)
  - layer 2: across switch ports
  - layer 3: round robin scheduling
- Provides load balancing and failover over the links
- Link Aggregation Control Protocol (LACP)
  - IEEE 802.3ad standard to negotiate bundled links between switches
- Packet reordering problem

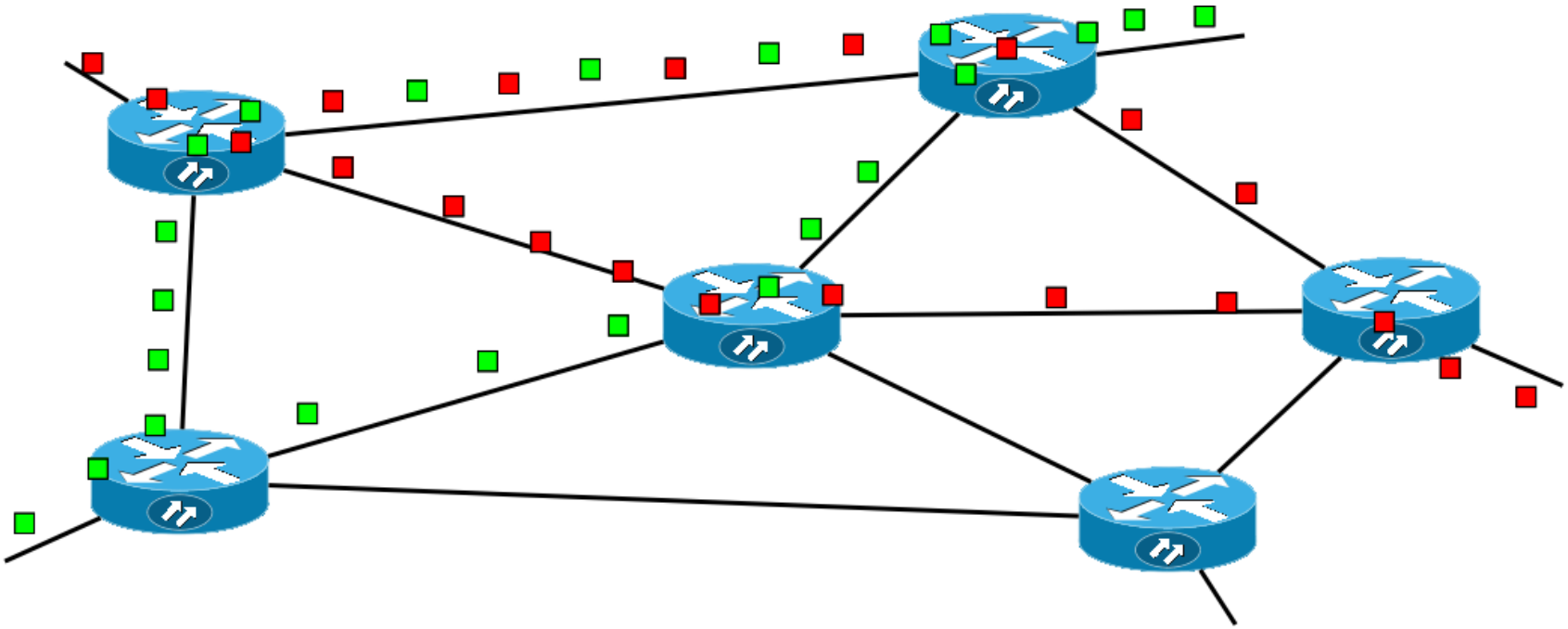
Link Aggregation—Proprietary Protocols

- Vendor's protocols
  - CISCO: EtherChannel and Port Aggregation Protocol
  - Juniper: Aggregated Ethernet
  - Nortel, AVAYA: Multi-Link Trunking family of protocols
  - Huawei: Eth-Trunk
- Linux Bonding driver
  - bonds several NICs into a logical channel
  - can work in active or passive mode
    - fault tolerance (both) and load balancing (passive)

Multipath Routing

- Benefits
  - fault tolerance
  - increased bandwidth
  - improved security
- Types of paths
  - overlapped
  - edge-disjoint
  - node-disjoint
- Problems with per-packet multipath routing
  - variable path MTU
  - variable latencies
  - packet reordering
  - debugging
- Equal-cost multipath routing (ECMO)
  - IEEE 8021Qbp (2014)

Multipath Routing—Picture



OLSR

- Optimized Link State Routing Protocol
  - RFC 3626
- IP routing for mobile ad hoc networks
- Basic principles
  - limited flooding: 2-hop neighbor
  - multipoint relays (MPR)
  - only MPR can source topology control packets
    - limits the extent of knowledge shared among nodes
    - not all links are advertised
  - no reliable algorithm
  - a pro-active algorithms: route computed before used

Reliable routing in MANET

- MANET a challenging environment for reliable routing
  - node mobility
  - limited battery capacity
  - low reliability of data transfer medium

  Reliable routing necessary for mobile ad hoc networks
- Basic principles:
  - proactive routing
  - reactive routing

Proactive routing in MANET

- Similar to routing in Internet
- Example: Destination Sequence Distance Vector (DSDV)
  - periodic exchange of routing information
  - independent of actual payload transport
- Drawbacks:
  - large number of control messages
  - high load on the network nodes
  - frequency must relate to the "mobility" of nodes within the network
    - can be very high or the routing info is obsolete
- Not really suitable for MANET

Reactive routing in MANET

- Reacts on data transfer needs
- Route discovery and Route maintenance
  - responsibility to find a route lies with the source node—discovery
  - every note detects topology changes
- Examples:
  - Dynamic Source Routing (DSR)
  - Ad-hoc On Demand Distance Vector Routing (AODV)
- Flooding mechanisms to discover the route(s)
- Naive approach: select the shortest path
  - suboptimal in MANET
  - creates congestion in the center of the network
  - "shortest" may not survive node mobility
- Multipath routing proposed as a better alternative

Multipath Routing in MANETs

- Several variants
  - delay aware protocols
  - reliable multipath protocols
  - minimum overhead
  - energy efficient
  - hybrid approaches
- Follow: Mohammed Tariquea, Kemal E. Tepeb, Sasan Adibic, Shervin Erfanib: *Survey of multipath routing protocols for mobile ad hoc networks*. J. Network and Computer Applications, Vol. 32(6), pp 1125–1143, 2009
  - `http://www.sciencedirect.com/science/article/pii/S1084804509001027`

Resilient overlay networks

- Introduced by Andersen:2001
- An architecture to support e2e communication to
  - detect network outages and performance degradation
  - recover from these

  and do it fast (in terms of seconds even when used over the Internet)
- An application layer overlay over the "standard" network
  - monitor the liveness and quality of Internet paths
  - take decision where to actually route each packet
- Optimizes application-specific routing metrics

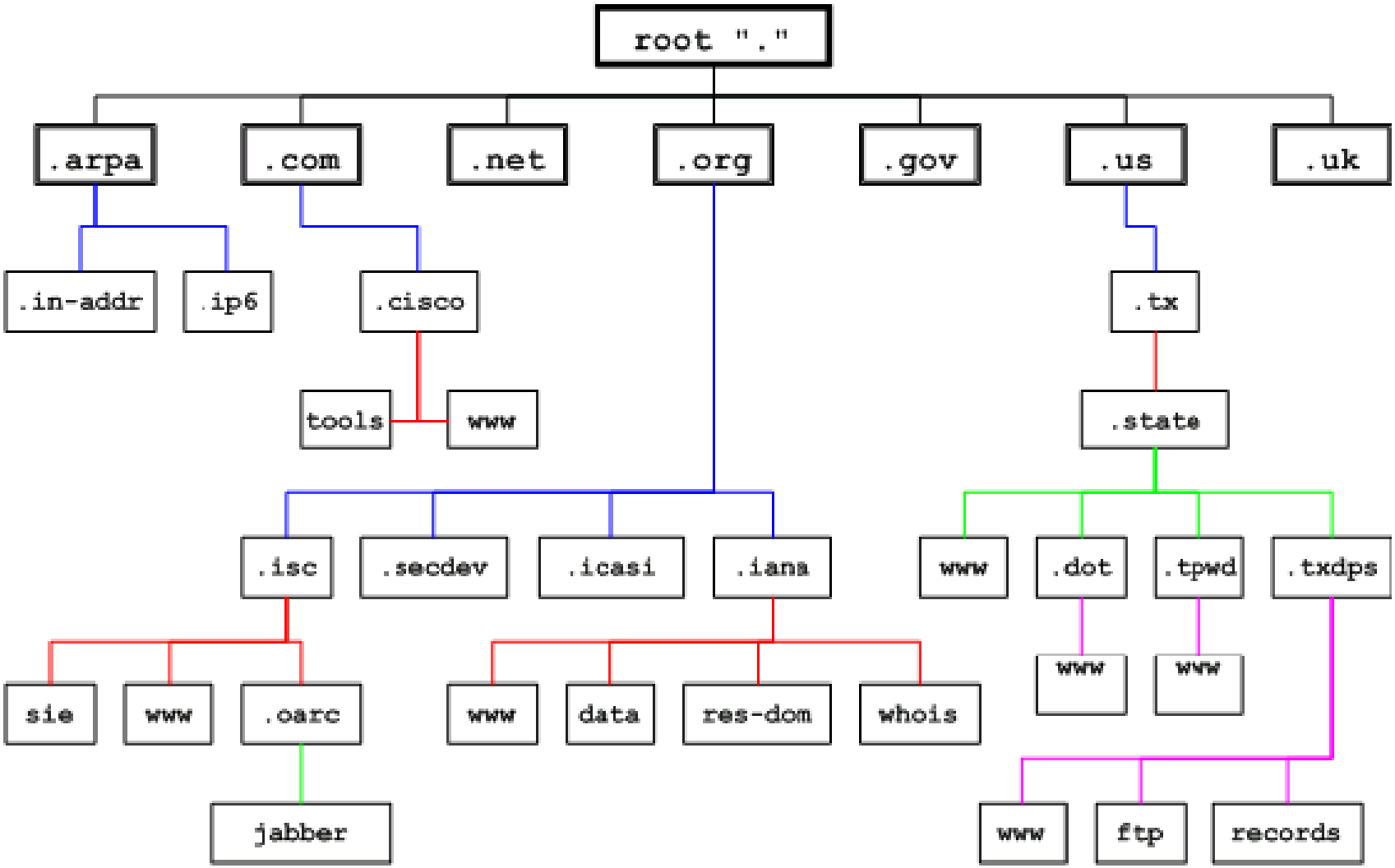
RON

- Some problems with "standard" routing
  - routing metrics are not modifiable by users
  - interdomain routing usually not too sophisticated
  - quality measurements usually only intra-domain
- RON concept
  - move routing to the end systems
    - but not to the applications
    - it is still a network
  - small scale (tens of RON nodes only)
  - independent end to end monitoring used for routing decisions
- Sophisticated applications (e.g. videoconferencing), but also coordinated reaction to DOS attack
  - cooperative defense
  - RON nodes used for
    - detection near malicious data target
    - traffic control near source
  - coordinated response through RON nodes

Domain Name Service (DNS)

- Associates host names with IP addresses
- Bidirectional
  - forward record: from host to IP address
  - reverse record: from IP address to host name
- Hierarchical distributed architecture
  - root servers
  - authoritative servers
  - data caching
- Specific vulnerabilities
  - Denial of service
  - information disclosure (reconnaissance before attack)
  - (authoritative) spoofing
  - cache poisoning

DNS Structure



DNSSec

- DNS security extension
  - uses PKI and digital signatures
- Server side
  - authentication
  - signed zone information
  - storage for public keys
  - signed query answers (A, MX, PTR)
- Client (resolver) side
  - origin authentication (authoritative)
  - data integrity
  - authoritative denial of existence

Summary

- Networks serving critical systems—the reliability of network as a whole becoming increasingly important
  - in some networks (e.g. MANET), the reliability is a necessary condition for proper operation
- Redundancy used as a standard engineering technique to achieve robustness
  - redundant systems more expensive
  - redundant systems more complex

  No "silver bullet" to solve the reliability requirement
- Presented examples of (more) reliable protocols
  - routing
  - resilient overlay networks
- Secure DNS as another example of the application of the basic principles
- Next lecture: Secure/Reliable data transport over the network