Internet infrastructure

Prof. dr. ir. André Mariën
Networking Essentials 1
Network architecture: layers

Component 1

Layer 0

Layer 1

Layer 2

Component 2

Layer 0

Layer 1

Layer 2

Virtual layer 2 link
Virtual layer 1 link
Real layer 0 link
OSI layers

- layer 7: application
- layer 6: presentation
- layer 5: session
- layer 4: transport
- layer 3: network
- layer 2: data link
- layer 1: physical
TCP/IP & Ethernet focus

• Focus on TCP/IP suite of protocols
  – Why?
    • Main protocols used for Internet
    • Available on all platforms and OSs

• Link level: Ethernet
  – All variants of ethernet protocols: wired, wireless
  – Why? Most common LAN technology
Network architecture: layers

Reasoning at one level without interference from others

Component 1

Layer 0

Layer 1

Layer 2

Component 2

Layer 0

Layer 1

Layer 2

IP

Ethernet

cable

Inter-layer Communication required

2011-2012
(c) A. Mariën
Simple network

• Simplest connection: only two systems
  – Point-to-point
    • Cross cable/null modem cable: connect two computers directly
    • Wireless: ad-hoc mode
    • Bluetooth: associate two devices (ex: laptop/GSM)
  – Implicit addressing possible
    • There is only one party on the other side
  – Need only data + error detection and correction
Local Area Network (LAN)

• All systems connected with each other
• Different topologies
  – Bus (not common for computer networks; a lot for communication inside computers)
  – Ring (not a lot anymore)
• All interconnected – virtually
  – All interconnected at IP level
  – But hub and spoke physically
LAN logical diagram

“bus”

Bus is security risk
Systems do not talk in private

“full interconnected”

System A
System B
System C
System D

System E
System F
System G

2011-2012
(c) A. Mariën
HUB

- Each component connected to HUB (port)
- HUB broadcasts packets on all other ports
- Typical use: network endpoints

HUB is security risk: SPoF + ideal MitM spot
Multiple HUBs

logical

physical

Sys a
Sys b
Sys c
Sys d
Sys e
Sys f
Sys g
Sys h
Sys i

2011-2012

(c) A. Mariën
Network basics: packets

- Considering packet-based communication
  - No permanent connection, no continuous bit stream, no long wire
    - Safe connection set-up is no guarantee for later safety
  - Rather: self-contained packets
    - Various forging options
  - Concept of connection is a ‘logical’ construction
    - Target of attacks
- Packet content:
  - “To” address
  - “From” address:
    - to be able to reply
    - To know who is sending
  - Bookkeeping
    - Sequence number of packet
    - Priority/urgency
  - Control
    - Integrity measures (against communication errors, not adversaries)
    - Data type
  - Data

- Initial assumption: friendly environment
- Pakkets can be destroyed, inserted, modified by all hops
- Pakkets can follow weird routes and still arrive
- Integrity: technical integrity only
Differences

• Addresses
  – Size of addresses
    • Fixed
    • Variable
  – Choice of addresses
    • Authorities - free
    • Collision issues
  – Address space organization
    • Flat – Structured
    • LAN – WAN - Worldwide

• Size of packets

• Over-fixation on efficiency and size should be over now

• Address structure is important for overall operation
  – Address management
  – Routing
  – complexity

• Authority governing addresses is powerful
LAN standards

• IEEE committee 802
  – 802.1: general issues
  – 802.3: Ethernet style
  – 802.5: token ring
  – 802.11: wireless (WiFi)

• Ethernet: CSMA/CD
  (Carrier Sense Multiple Access with Collision Detection)
Ethernet physical connections

- **10Base5:**
  - coax-cable, thick ethernet (0,5 inch)
  - connections: hardwired on the cable
  - maximum: about 200 devices
  - maximum distance: about 500m

- **10Base2:**
  - coax cable, thin ethernet (0,2 inch)
  - connections: hardwired on the cable
  - maximum: about 30 devices
  - maximum distance: about 185 meter

- **10BASE-T, 100BASE-T, 1000BASE-T:**
  - twisted pair-kabel, RJ-45 connectors
  - 10 Mbps, 100Mbps, 1Gbps
  - point-to-point (two end-points)
  - maximum distance: about 100 meter
Packet essentials:
- (fromAddress, toAddress, data)

Ethernet addresses: MAC (48 bit)
- MAC addresses are assigned to Ethernet devices by the manufacturer.
- The manufacturer gets a block (or more) of MAC addresses he can use.
- Therefore there should never be a conflict of addresses.

It is possible to change the MAC address, either inside the hardware or in the software.
- It depends on the system how easy it is to reconfigure the MAC address.
- Whether this is a good idea is another question.

An Ethernet packet has a maximum payload of 1500 bytes.
There can be a maximum of 1024 interfaces on one Ethernet segment.
- So ethernet address could be very small
- Large space avoids conflicts, is management driven

The ethernet addresses inside a network have no structure
- Filtering and routing on an individual basis
- Could be set and used as an identifier inside the organization, but limiting portability
Three types of communication:

- Three types:
  - Directed (unicast): single destination
  - Broadcast: all on the (Ethernet) segment
  - Multicast: subset of systems
    - Possibly overlapping subsets of the systems
    - A form of publish-subscribe:
      - Systems register for multicast communication
      - Publishers publish to any registered listeners

- Note:
  - The technology itself assumes a form of broadcasting, so the other communication methods are logical methods
    - Unicast is not private
    - Unsubscribed nodes still could see the multicast messages
  - The type is determined by the address
    - A part of the address space is reserved for multicast and broadcast.
    - See http://www.iana.org/assignments/ethernet-numbers
    - Both “from” and “to”
Promiscuous mode

• Ethernet cards typically filter the traffic:
  – Broadcasts: ok
  – Multicasts: for which there is a subscription
  – Packets with its own MAC address as destination

• In some cases it is necessary for a machine to listen to all traffic:
  – The cards support this mode of operation: ‘promiscuous’ mode
  – This mode can also be abused to listen in to other peoples communication

• Tool: wireshark
  – http://www.wireshark.org/
Switch: why?

• The number of components on network segment is limited
  – network congestion
  – token ring: length of ring

• Traffic limitations:
  – bandwidth is limited
  – \( n \) out of \( m \) systems with heavy interaction influence all interactions
Switch properties (IEEE 802.1d)

• IEEE standard 802.1d lists three main properties:
  – Store and forward
  – Learning cache of MAC addresses
  – Loop avoidance: spanning tree computation
Ethernet switch

MAC1: P1
MAC2: P1
MAC3: P2
MAC4: P2
MAC5: P3
MAC6: P3

D1
MAC1

D2
MAC2

D3
MAC3

D4
MAC4

D5
MAC5

D6
MAC6
Ethernet switch: port learning

MAC1: P1
MAC2: P1
MAC3: P2
MAC4: P2

D1 => D4
D2 => D1
D3 => D2
D4 => D2
Switch: learning

Switch DB:

1. P1: MACc1
2. P2: MACc2
3. P3: MACc3

c1: MACc1 MACc2

p1

p2

p3

c2: MACc2 MACc1

c3: MACc3 MACc2
Switch: spanning tree

- Problem: loops in switched networks
- Different from IP router loops: one packet starts looping
- Switch: packet multiplication possible
- Solution: algorithm to compute spanning tree
Example network

From book: Interconnections
Loop free

From book: Interconnections
STP

• Goal
  – Determine Root Bridge
    • Will be the key bridge: all systems can connect to it (indirectly) hence spanning
  – Determine Designated Ports per switch
    • Ports that packets will be forwarded on (broadcasts/unknown MAC)
  – Determine port with best path to root bridge
    • Best: measure for instance hop count

• How?
  – Send inter-switch configuration messages (not forwarded on other ports) = per physical LAN
  – Message carrier
    • Protocol message via ethernet multicast
  – Message contains
    • Switch ID, port ID
    • Path to Root bridge & cost
STP

• Algorithm
  – Send initially on all ports:
    • Own ID as Root bridge, cost 0
  – Fixed point computation:
    • Use (root bridge, cost, transmitter) as number
    • Lower is better
  – Only send if you have a “better” message to send on the port than the one you received

• Convergence
  – Lowest switch number known by all switches
  – Cost to Root bridge known via all ports
  – Information per port if you are the closest on that physical LAN to the Root bridge (you are the Designated switch on that physical LAN)
Costs

From book: Interconnections
Port configuration

From book: Interconnections

What can a rogue participant do?
IPv4
IP layer

• IP layer:
  – Basic layer for TCP/IP networking
  – Carrier for the ‘Internet’
  – Independence of physical networking
  – Available on practically any system today

• Packet essentials:
  (from address, to address, data)
  – From/to: 32 bit address: IPv4 address
  – Additional info:
    • version, lengths, checksum, flags, fragmentation info
    • time-to-live, higher level protocol (ICMP, UDP, TCP)
IPv4 addressing

• IPv4 address is 32 bit number
  – typical writing: 4 digits, each 0-255
    (hexadecimal: 0x00 - 0xFF)
    “dotted decimal”: d1.d2.d3.d4
  – example: 206.4.56.11 = 0xCE04380B

• Each component has a unique address
  – Sufficient when all nodes connected to the same LAN
  – “worldwide unique” addresses
    • Structured
    • Regulated
Multiple LANs

• Within each LAN: operation similar to single LAN
  – Component addresses must be unique

• Inter-LAN:
  – Router(s): systems that have an address on both LANs
  – They “know” when to send a packet from one side to the other
  – Decision based on addresses (simplicity)

• Component address:
  – Split in network number and component number
  – Address is a tuple: (LAN, component)
Routers
Router between two LANs

- Router is connected to two LANs: LAN1, LAN2
- Packets from one LAN to another: must pass through the router
- Router has a different address on both LANs
- All machines know the address of the router
  - in LAN1: (LAN1,R1)
  - in LAN2: (LAN2,R2)
- All machines know if IP address is local to their LAN
LAN

• Lan determination
  – LAN address: first n bits
  – Old style: first 8, 16, 24 bits (class A, B,C,D network)
  – Network mask:
    • (address & mask) = network address
  – Example:
    • mask: 255.255.255.0 = 0xFFFFFFFF00
    • network address: 206.4.56.0
    • possible nodes: 255

• LAN determination: general
  – CIDR: Classless Inter-Domain Routing
  – network part: first n bits, n any
  – Example:
    • network mask: 255.255.255.240
    • IP address: 206.4.56.11
    • number of nodes in network: 16
    • two special addresses: all ‘0’, all ‘1’
      all ‘1’ broadcast address: 206.4.56.15
    • actual real nodes possible: 16-2 = 14
Host addressing principle
Host addressing principle (cont.)
Host addressing principle (cont.)
Host addressing principle (cont.)

(C1, LAN1) -> (R, LAN1) -> (C2, LAN2)

(c) A. Mariën
Network with multiple LANs and routers

• Component C1 wants to send packet to component C2

• C1 is on LAN1, C2 on LAN2

• C1 must decide:
  – LAN2 == LAN1 ? Local connection: obtain MAC and send
  – LAN2 <> LAN1: find right router
    • router with list of paths
    • default router
Switches revisited
Virtual LANs
Virtual LANs

Problem

• subLAN: organized by:
  – organizational unit: admin, HR, development
  – physically close: floor 1, floor 2, building A
  – security realm: management, R&D

• These requirements are conflicting

• IP LAN requires IP numbering convention

Solution

• Approach:
  – Separation of
    • physical connection topology
    • logical topology
  – Flexibility
    • logical LAN reconfiguration without physical reconfiguration

• How:
  – Create Virtual LAN
    • Single broadcast domain
    • Packet sniffing: within VLAN only
    • VLAN: one IP subnet
VLAN: possible configurations

• Port based: 1-i, i+1-j, j+1-n: 4 VLANS
• Port per port: which VLAN
• VLAN/MAC mappings
  – Assign VLAN based on observed source MAC
• VLAN/IP net
  – Assign VLAN based on source IP
VLAN: diagram

physical

logical

(c) A. Mariën
VLAN + router

physical

logical
Additional functions

• Private VLAN
  – The nodes cannot communicate between them, only with configured ports/addresses
    • When is this useful?
    • What is the alternative?
    • How can this be done?

• Tagged VLAN
  – VLANs over one wire: the packets are extended with a tag, indicating the VLAN they belong to
  – Can be used without switches
    • When is this useful? What is the alternative?
  – Allows switches to extend VLANs across single, long distance wire (typically fibre)
Switch creates logical networks

Configuration change
Span port

- Sometimes: need to see all traffic over all VLANs
  - Examples: network and security monitoring
- Solution: dedicated port that gets all traffic: Span port
- Potential bottleneck: ALL traffic
- Fasted technology required
- Expensive
Trunk

Packets in the VLAN are tagged
Connecting Switches
Virtual interfaces

Packets in the VLAN are tagged
Real and virtual interfaces

IP1
Netmask1

logical interface

Physical interface

tagged packets

Physical interface

logical interface

IP3
Netmask1

IP2
Netmask2

logical interface

Physical interface

logical interface

IP4
Netmask2
VLAN classes

• Default VLAN
  – All ports are by default member of the default VLAN

• Data VLAN (aka user VLAN)
  – switch management: separate user data

• Native VLAN
  – Assigned to an 802.1Q trunk port
  – The 802.1Q trunk port places untagged traffic (traffic that does not come from a VLAN) on the native VLAN

• Management VLAN
  – any VLAN to access the management capabilities of a switch
  – Do not use default VLAN

• Voice VLAN: to carry voice traffic
  – Priority over data
  – Data intensive service
Networks

Router
Switch
HUB
sys

Router
Switch
HUB
sys
Ethernet - power

• Ethernet over power
  – Use power wiring
  – Plug in specific adaptors
  – Mind different phases!

• Power over ethernet
  – Used mainly for two types of devices
  – Wireless access points
  – VoIP telephones
  – Power consumption switch: changes