# OSI model and ISIS

Pehr Söderman
KTH-NOC/CSC/NADA
Pehrs@kth.se

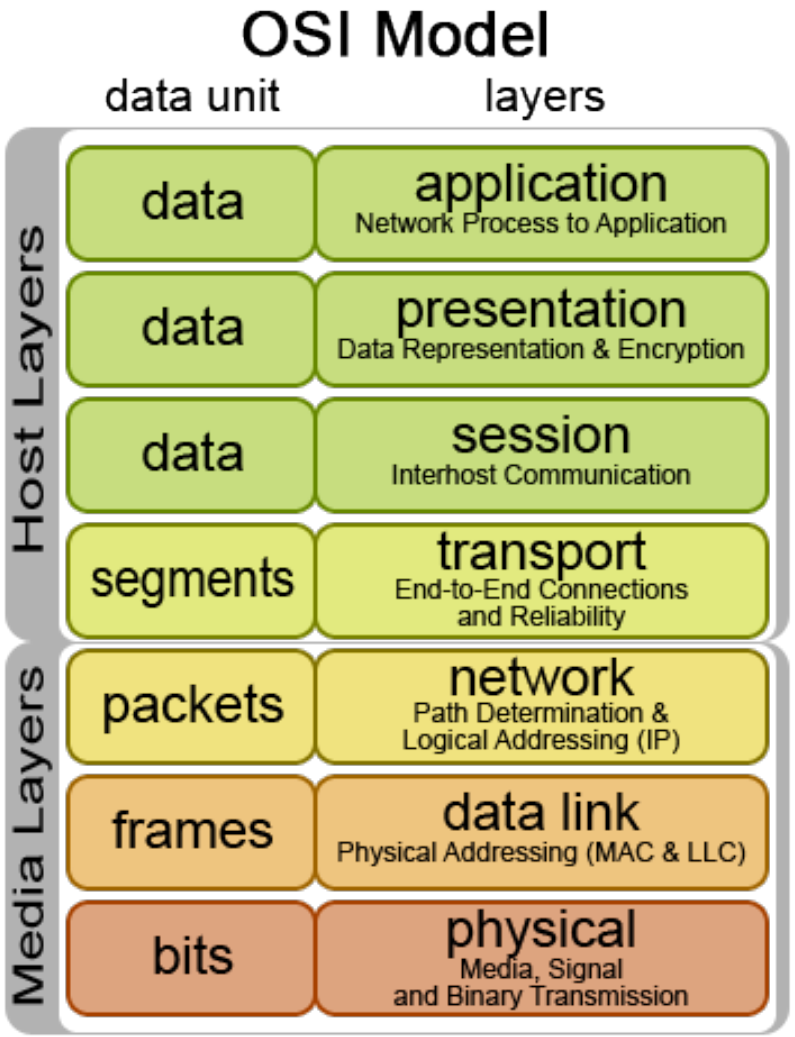
# In the begining there were many protocols

- Banyans VINES Internet Protocols (VIP)
- Xerox network system (XNS)
- IBMs DECnet
- Apples AppleTalk
- Novells Internetwork Package Exchange (IPX)
- And talking to your neighbours was impossible

# Fundamental idea of OSI

- Define a stack of 7 layers
- Create new protocols for each layer
- Replace the many vendor specific protocols
- Bring the world into the internetwork age
- Where did it all go so very wrong?

# The OSI stack




- The most important fundamental result of the OSI project
- You should know this, by heart.

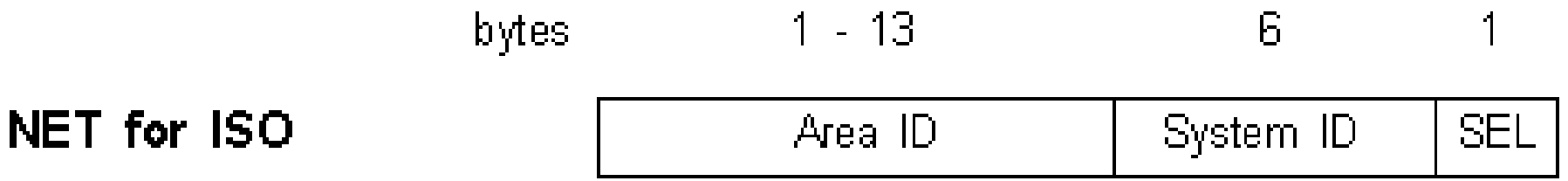
# A vocabulary of OSI terms

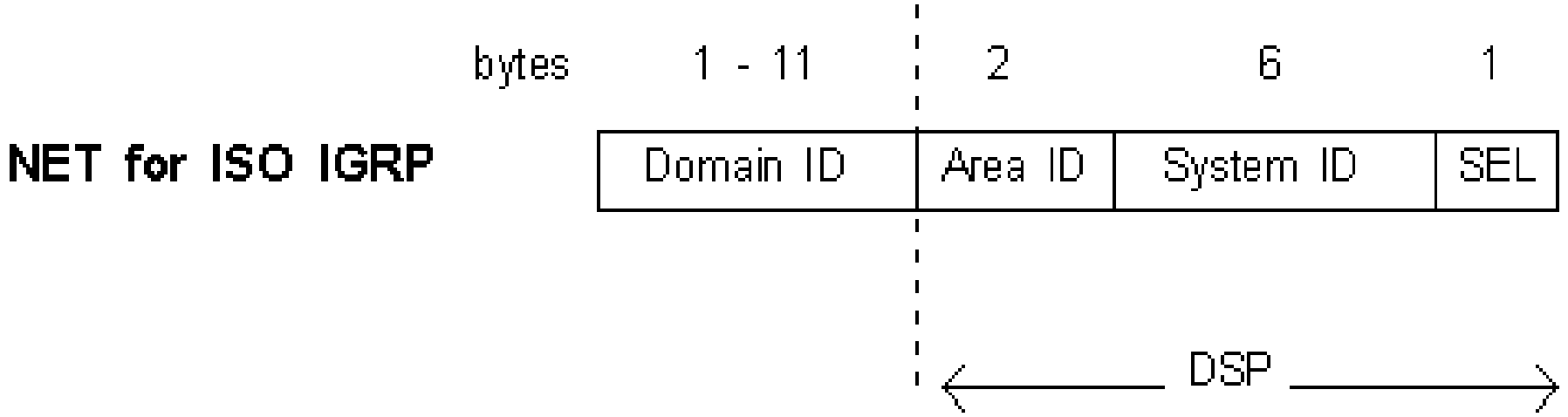
- IP
- ICMP
- ARP
- Router
- Host
- Packet
- CLNS
- CLNP
- ES-IS
- IS (Intermediate system)
- ES (End System)
- PDU (Protocol data unit)

# ISO adressing

- Addresses are 6-20 bytes (48-160 bits)
- Addresses are structured
- Addresses belong to a network node, not a link or interface
- Addresses come from some kind of administrative domain

# ISO addresses



# ISO addess parts

- AFI (Authority Format Identifier)
  - Specifies the format of the rest of the adress
- IDI/ICD (Initial Doman Identifier/International Code Designator)
  - Speficies the authority for the adress space
- HO-DSP (High Order Domain Specific Part)
  - Indicates the sub authority for the routing domain
- Area
- System ID

# Network Entity Title (NET)

- Nsel = 0
- Each router have atleast one NET
- It contains:
  - Area ID
  - System ID
  - Selector (must be 0)

# Example of NET adress in .se

- AFI (Authority Format Identifier) 39
- IDI (Initial Domain Identifier) SE 752
- DFI (Domain Format Identifier) 100
- AAI (Administrative Authority Identifier) 0014
- RSVD (Reserved)
- RD (Routing domain)
- Area, System ID and sel

| AFI | IDI | DFI | AAI | rsvd | RD | Area | System ID | Sel |
|---|---|---|---|---|---|---|---|---|
| 39 | 752f | 0100 | 0014 | 0000 | 0001 | 0001 | 1921.6800.1001 | 00 |

# IS-IS background

- Created to support CLNP (Connectionless network protocol)
- To support transition from IP to OSI Integrated IS-IS was created
- Integrated IS-IS can operate in pure CLNS, pure IP or mixed networks
- CLNP/CLNS are defined in ISO 10589
- Integrated IS-IS is defined in RFC 1195 (Proposed)
- I will simply say ISIS

# Common functionality with OSPF

- Both are Link State and use the Djikstra algorithm
- Both have a hello packet system
- Both have a two level routing heirarchy
- Both can do summarization
- Both are classless
- Both use DR on broadcase networks (DIS)
- Both have authentication support

# ISIS is very popular in the ISP world

- Major ISP tends to use ISIS instead of OSPF
- Sunet
- Nordunet
- Tele2
- Sprint
- Etc.

# ISIS protocol

- ISIS is NOT an IP protocol
- ISIS can not even run over CLNP
- ISIS runs directly on the Data link layer
  - Conceptionally clean
- Security advantages?
- ISIS uses TLV encoding

# ISIS Packets

- All ISIS packets starts with a common header
- Followed by a packet specific header
- Followed by (optional) packet data
- Three common types
  - Hello
  - LSP (Link State PDU)
  - SNP (Sequence Number PDU)
    - CSNP (Complete Sequence Number PDU)
    - PSNP (Partial Sequence Number PDU)

# Hello protocol on P2P links

- Use the ES-IS protocol to contact neighbours
- If we get an IS Hello back, send ISIS Hello
- Set the Level 1/2/1+2 in the ISIS Hello packet
- Continue sending Hello every 9 seconds
  - 3 lost packets=link down
- Pad to full MTU size (Why?)
- No checksum on layer 3

# Hello protocol on multicast networks

- Send ES-IS Hello
- Send ISIS Hello, do not wait for IS-Hello
- Create a neighbours connections for each L1 and L2 adjacency
- Use multicast!
  - AllL1ISs (0180.c200.0014)
  - AllL2ISs (0180.c200.0015)
- Connection keepallive identical to P2P links

# Connections on multicast networks

- Connection to everybody with the same Level
- Fully meshed!
  - Unlike OSPF
- Still we elect a Designated IS

# How do we synchronize the DB?

- Send CSNP to show your DB
  - Complete sequence Number PDU
- Send PSNP to request LSP
  - Partial Sequence Number PDU
- Send LSP as response to PSNP
- Compare to OSPF!

# Database updating

- Each router is responsible for its links
- Each router announces information about its links to all neighbours
- Each router forwards every LSP
- Each LSP is acked with a PSNP
- Incremental updates
- Periodic updates
  - Max life is 1200 seconds, periodic updates after 15 min +-25%

# Flooding on P2P nets

- The router sends one or more LSP
- The neighbour responds with an PSNP
- If the neighbour hasn't responded in 5 seconds retransmit

# Flooding in multicast networks

- Familiar problem with n*(n-1)/2
- We need to turn it into P2P links for Djikstra anyway.
- Create a pseudo node, report a link to the pseudo node.
- DIS announces the pseudonode, metric to all neighbours is 0.

# Flooding in multicast networks

- DIS sends a CSNP to all neighbours every 10 seconds
- Reciever compares its database with the CSNP
- If the reciever has a missing LSP or have a newer it sends it to everybody.
- If the reciever lacks an LSP it sends a PSNP to the DIS

# Electing DIS

- Highest priority
- Highest Router-ID/System-ID
- If a new router joins with a higher priority the election is redone.
- The DIS creates the LAN-ID by combining its own system-ID with a pseudonode ID
- Only one DIS
- No state in DIS
- No backup DIS (Why is it not needed?)

# Common data in LSP

- PDU Length (Octets)
- Remaining Lifetime (Seconds)
- LSP ID (SystemID + PseudonodeID + frag num)
- Sequence number (32 bits)
- Checksum (End to end)
- P (Partition repair)
- ATT (Attached: Error, Expense, Delay, default metric, used for default routes)
- OL (Overload, we will get to this later)
- IS Type (L1, L2, L1/L2)

# When is a new LSP created?

- Adjacency up or down
- Interface up or down
- Redistribution changed
- Inter-area routes changed
- Metric changed
- Period changed
- Timeout
- Configuration changed...

# How do we handle a new LSP

- Compare it with the LSPDB. If newer
  - Install it in the LSPDB
  - Ack with a PSNP
  - Flood to all neighbours
  - Run SPF
- If older
  - Ack with PSNP
  - Send our version of the LSP
  - Wait for PSNP
- If same age

# Overload bit

- Also known as ”Hipety” or ”Broken” bit
- If the IS lack memory to store the full table it can set this bit
- The router is then not used to transit traffic, but may still forward to directly connected nets
- It is sometimes set manually to get the same effect
- May be used in BGP/IGP interaction

# IS-IS areas

- Two levels, similar to OSPF
- L1 knows only about it's own area and border routers
- L2 is the backbone area
- L2 may not be partitioned
- L1/L2 forwards the ATT-bit into the L1 area. It functions as the default router.

# Partition repairs

- Used to prevent paritions of the L1 area
- Similar to the virtual link in OSPF
- Two L2 routers form an L1 virtual link between the partitioned L1 areas

# Route leaking

- ISIS can result in suboptimal routing
- Allow an L1/L2 to leak L2 information into L1
- Can only be done if the route is in the table of the L1/L2 router
- Creates a form of NSSA

# Decision process

- L1 and L2 have completely separate trees
- 4 metrics (Usually only 1 is used)
  - Default
  - Delay
  - Expense
  - Error
- L1 routes have higher priority
- L2 have both internal and external routes
- Load balancing is done when several routes have the same metric(s)

# ISIS header

- Protocol Identifier (0x83)
- Header Length (8 bytes, fixed, same as CLNP)
- Version (0x01, fixed, for future use)
- ID length (Size of the ID part of the NSAP add)
- Type (Following packet type)
- Version (Copy of previous field)
- Reserved (0x00)
- Maximum Area Addresses (Limits the number of area addresses an IS can belong to)

# Hello header fields

- Circuit type (Defines L1/L2/L1+2)
- Source ID (ID of the sender)
- Holding Time (Minimum timeout)
- PDU Len (Of following packet)
- Local Circuit ID (Circuit ID of the router)
- Priority (0-127, for DIS election, multicast only)
- LAN ID (System ID + 1 octet, multicast only)

# Interesting TLV encoded fields

- Area adress
- Padding
- Authentication
- Protocols Supported
- IP interface adress
- 3-way handshake
- Intermediate System Neighbours (multicast)

# CSNP
# (Complete Seqence Number PDU)

- Header:
  - PDU Length
  - Source ID
  - Start  LSP ID
  - End LSP ID
- TLVs:
  - LSP entries (Summary of known LSP)
    - LSP ID, Sequence number, Checksum, Lifetime
  - Authentication

# PSNP
# (Partial Sequence Number PDU)

- Header:
  - PDU Length
  - Source ID
- TLVs
  - LSP entries (Summary of requested LSP)
    - LSP ID, Sequence number, Checksum, Lifetime
  - Authentication

# OSPF vs ISIS: Encapsulation

- OSPF runs over IP
  - Allows virtual links
  - Relies on fragmentation if we hit MTU
  - Vulnerable to spoofing and DoS
- ISIS runs over MAC
  - It's a clean solution
  - More difficult to spoof and attack
  - Harder to implement

# OSPF vs ISIS: Encoding

- OSPF uses ”efficient” coding
  - Positional fields
  - 32 bit alignment
  - Only LSA can be extended
  - Unknown LSAs are discarded
- ISIS uses TLV
  - No alignment
  - Extensible by its very nature
  - Unknown LSAs are flooded
  - Nested TLV gives a lot of flexibility

# OSPF vs ISIS: Areas

- OSPF have area boundries inside routers
  - Routers in many areas
  - Routers must calculate SPF per area
- ISIS have area boundries on links
  - Router is in one area and, perhaps, the backbone
  - Biased towards large areas
  - Historically been badly deployed
  - ISIS seems to handle large areas very well

# OSPF vs ISIS LSADB

- OSPF Stores Database Advertisements
  - LSAs are usually many and small
  - Network and Router LSA can get large
  - LSAs are grouped in LSUpdates for flooding
  - LSUpdates need to be rebuilt for each hop
- ISIS stores LSPackets
  - LSPs are organized by the originating router
  - LSPs are always flooded intact, never changed
    - We need the same minimum MTU in the whole network!
  - Each topology change gives a new LSP

# OSPF vs ISIS Database syncing

- OSPS have a complex procedure
  - Minimizes transient routing problems
  - Majority of the implementation complexity
- ISIS uses the usual flooding
  - Larger risk of transisent problems
  - Easy to implement

# OSPF vs ISIS Scalability

- OSPF is limited by Router and Network LSA size (max 64k or O(5000) links)
  - External and interarea routes have no real limit
- ISIS is limited by LSP count (256 fragments * 1470 bytes)
  - Can be bypassed by using hacks
- If you run into these your network topology is beyond insane

# OSPF vs ISIS Extendability

- OSPF was never built to be extended
  - Proudly optimized for IPv4
  - No room for new protocols
  - IPv6 will require a new protocol (OSPFv3)
- ISIS is inefficient but extendable
  - So far extending ISIS has been suprisingly painfree
  - IPv6 ready (just like it's IPv4 and IPX ready...)

# OSPF vs ISIS Conclusions

- For all but insane topologies they are functionally identical
- Stability and scalability are mostly a matter of hardware, software and topology, not protocol
- Choose the one you are most comfortable with
- If you are running IPv6 give ISIS a closer look...