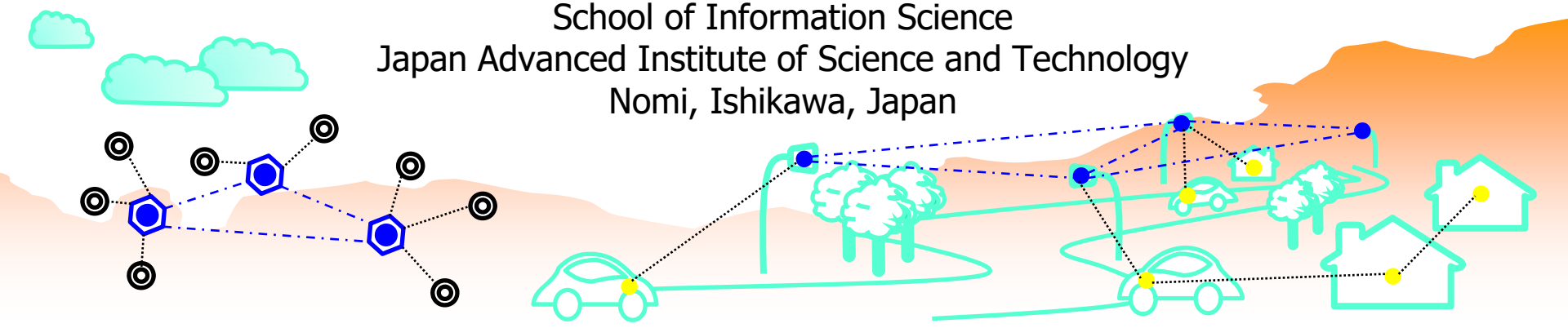
I226
Computer Networks

Chapter 12

Design, Implementation, and Operation of Network Systems

Assoc. Prof. Yuto Lim

School of Information Science
Japan Advanced Institute of Science and Technology
Nomi, Ishikawa, Japan

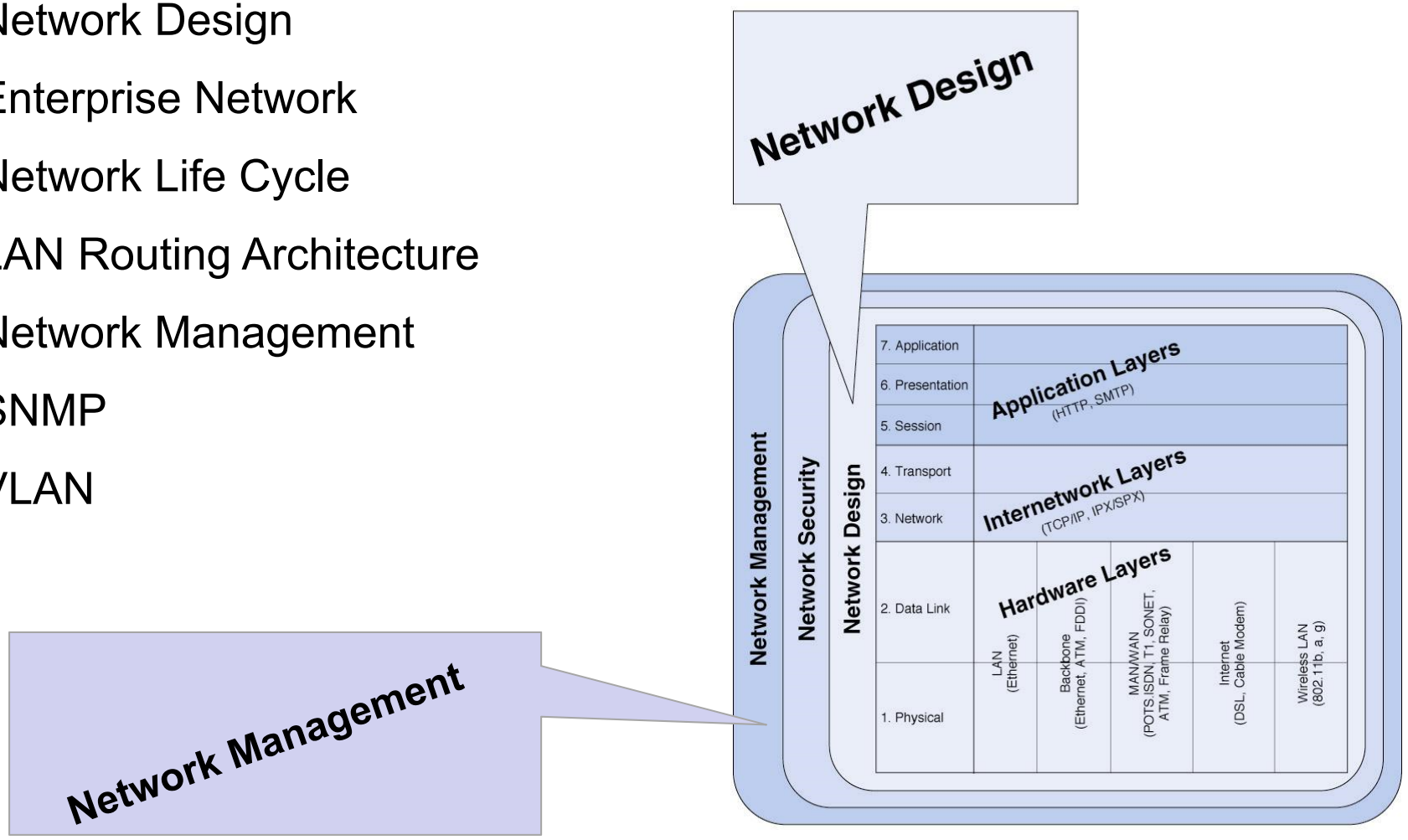


Objectives of this Chapter

- Explain the network design and network life cycle
- Explain the entry aggregation technique for routing table
- Provide the knowledge on how to plan for a bandwidth for a network
- Give a basic knowledge on how to design the router architecture
- Give an understanding what is the basic of network management
- Explain the operational model of SNMP and its protocol functions
- Provide the knowledge of VLAN technology and show that a trunk can transport both tagged and untagged VLANs
- Illustrate and discuss a VLAN configuration

Outline

- Network Design
- Enterprise Network
- Network Life Cycle
- LAN Routing Architecture
- Network Management
- SNMP
- VLAN



Traditional Network Design

- Traditional network design approach follows a structured systems analysis and design process similar to that used to build application systems
  - Network analyst meets with users to determine the needs and applications
  - Network analyst estimates data traffic on each part of the network
  - Network analyst designs circuits needed to support this traffic and obtains cost estimates
  - Finally, a year or two later, the network is implemented
- 3 forces are making the traditional network design approach less appropriate for many of today's networks
  - Underlying technologies used in computers, networking devices and network circuits are rapidly changing
  - Network traffic is growing rapidly
  - Balance of costs has changed dramatically over the last 10 years

Network Design: Building Block

- While some organizations still use the traditional approach, many others use a simpler approach to network design, the building block approach
- This approach involves three phases: needs analysis, technology design, and cost assessment
- When the cost assessment is initially completed, the design process returns to the needs analysis phase and cycles through all three phases again, refining the outcome of each phase
- Process of cycling through all three design phases is repeated until a final design is decided on

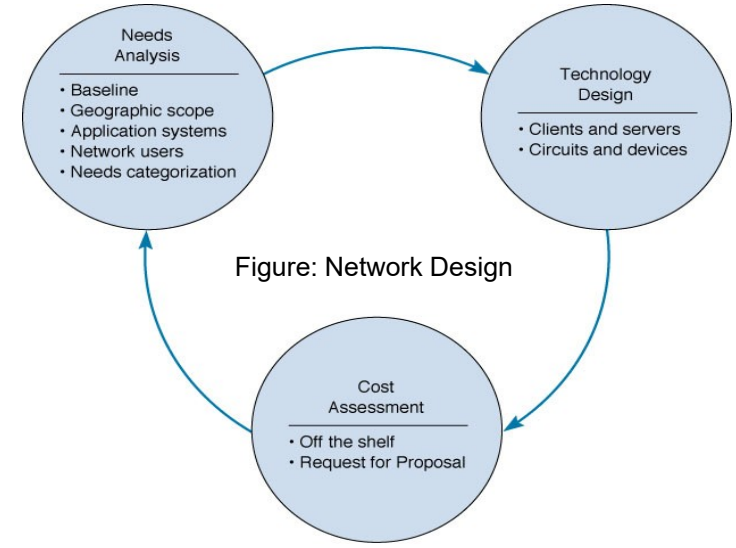
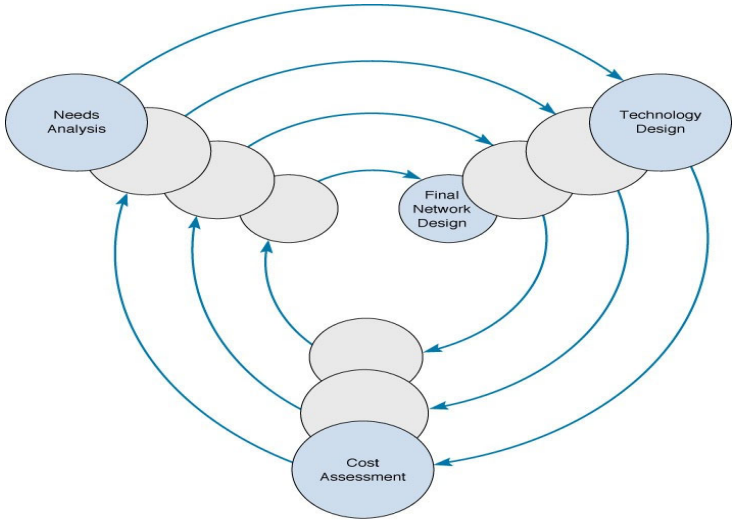
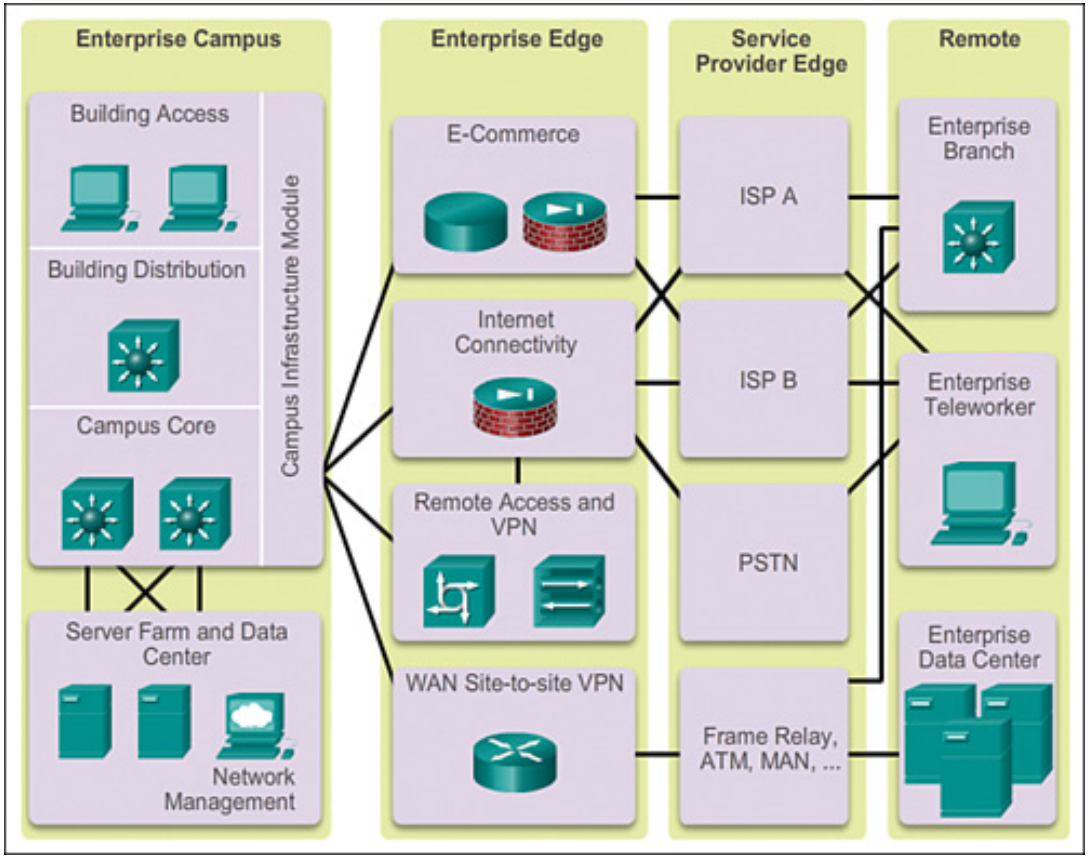


Figure: Network Design



Enterprise Network Architecture

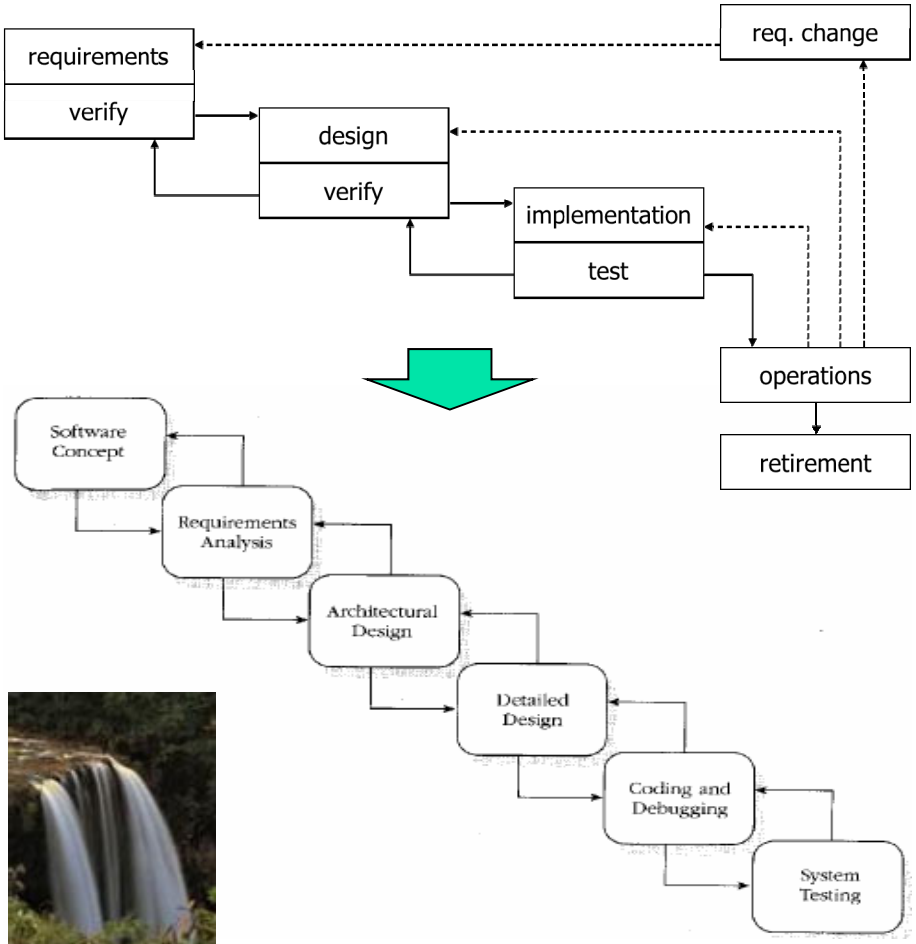
- Enterprise Campus interconnects the group of networks (LANs) over single geographic area
- Enterprise Edge aggregates the connectivity from various areas (e-commerce, Internet connectivity, VPNs) and routes the traffic into campus core
- Service Provider Edge provides Internet, PSTN and WAN services
- Remote has branch, teleworker, and data center
  - **Branch** extends networks to a small group of branches
  - **Teleworker** connects individual users to network resources remotely
  - **Data Center** manages centralized data systems for the entire enterprise

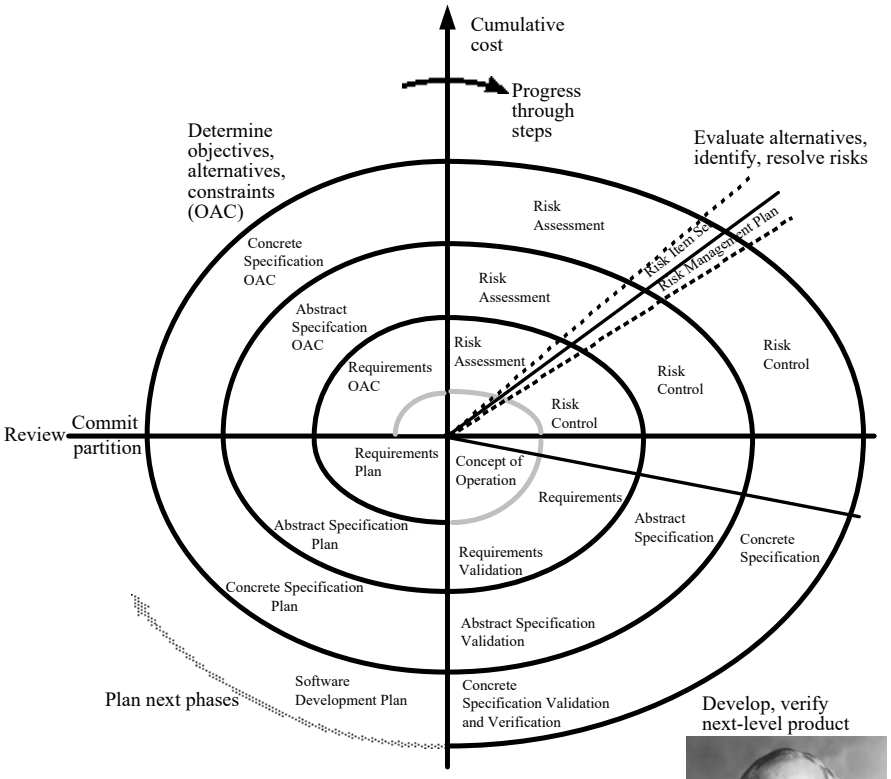


Network Implementation and Life Cycle

- To implement a new network or replacing an existing network, we use network life cycle approach
- Network life cycle
  - Process of creating a new network or changing an existing network
  - Provides a comprehensive framework against which network managers can make critical decisions, whether in moments of immediate crisis or for long-range planning
  - Defines a range of needs that require a variety of methodologies and tools for network performance management
- Network life cycle type
  - Waterfall cycle works "flows down" from one stage into the next. After the network is deployed, the life cycle begins again for the next update
  - Spiral (whirlpool) cycle is a variation of the waterfall cycle. The spiral cycle can adapt quickly to new requirements. This is accomplished by looping through all stages several times with a shorter time
  - Others: code-and-fix, structured evolutionary prototyping, dynamic systems development method (DSDM), design-to-schedule

Waterfall and Spiral (Boehm)





Barry Boehm
University of Southern California

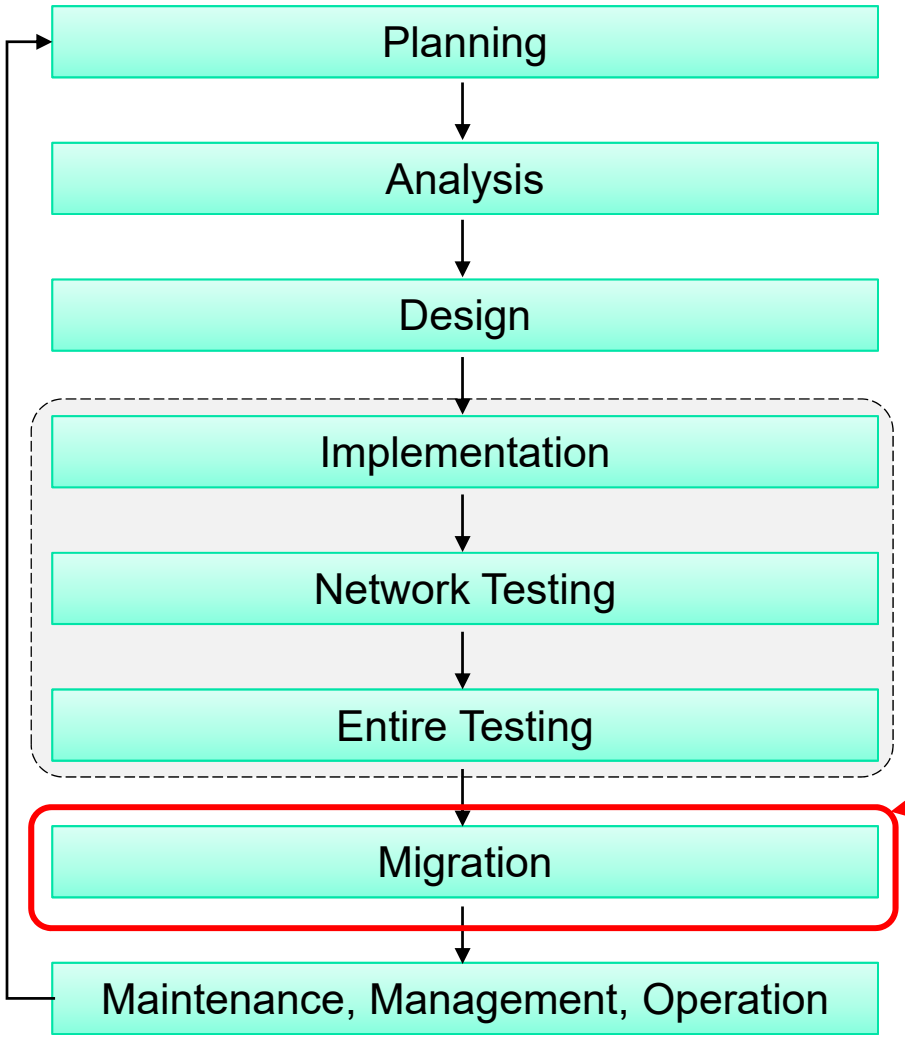
Comparison

	Waterfall	Spiral
Strengths	• Easy to understand, easy to use • Provides structure to inexperienced staff • Milestones are well understood • Sets requirements stability • Good for management control (plan, staff, track) • Works well when quality is more important than cost or schedule	• Provides early indication of insurmountable risks, without much cost • Users see the system early because of rapid prototyping tools • Critical high-risk functions are developed first • The design does not have to be perfect • Users can be closely tied to all lifecycle steps • Early and frequent feedback from users • Cumulative costs assessed frequently
Weaknesses	• All requirements must be known upfront • Deliverables created for each phase are considered frozen – inhibits flexibility • Can give a false impression of progress • Does not reflect problem-solving nature of network/protocol development – iterations of phases • Integration is one big bang at the end • Little opportunity for user to preview the system (until it may be too late)	• Time spent for evaluating risks too large for small or low-risk projects • Time spent planning, resetting objectives, doing risk analysis and prototyping may be excessive • The model is complex • Risk assessment expertise is required • Spiral may continue indefinitely • Developers must be reassigned during non-development phase activities • May be hard to define objective, verifiable milestones that indicate readiness to proceed through the next iteration

Comparison (cont.)

	Waterfall	Spiral
When to use	• Requirements are very well known • Product definition is stable • Technology is understood • New version of an existing product • Porting an existing product to a new platform	• For large, expensive, and complicated projects • For medium to high-risk projects • New product line • When creation of a prototype is appropriate • When costs and risk evaluation is important • Long-term project commitment unwise because of potential changes to economic priorities • Users are unsure of their needs • Requirements are complex • Significant changes are expected (research and exploration)

Network Life Cycle



Clarification of the concept, target determination, organize requirements

Traffic analysis, topology design, applied technology choice, basic design bandwidth, network configuration design, equipment selection

Detailed design bandwidth, addressing scheme, implementing design, parameter design

Cabling, equipment installation, equipment configuration, unit testing equipment

Communication test, traffic load test, backup and fault tolerant test

Additional test, including the application-level communication, performance evaluation, and server

ONLY different

Switching to a new network (entire replacement, partial replacement)

Traffic monitoring, resource management, information storage failure

* Please see the same life cycle, Chapter 11, no. 5

Advantages of Life Cycle Approach

- Lower costs
  - Reduce cost for infrastructure changes and resource waste
  - Reduce operating expenses by improving the efficiency of operational processes and tools
- Improve high availability
  - Specifying the correct set of hardware and software releases, and keeping them operational and current
  - Producing design operations and validating network operations
  - Proactively monitoring the system and assessing availability trends and alerts
- Gain business agility
  - Establishing business requirements and technology strategies
  - Integrating technical requirements and business goals into a detailed design and demonstrating that the network is functioning as specified
- Accelerate access to network applications and services:
  - Assessing and improving operational preparedness to support current and planned network technologies and services
  - Improving service-delivery efficiency and effectiveness by increasing availability, resource capacity, and performance

Network Planning and Design

- Network is a foundation infrastructure for the organization activities of a campus or an enterprise
  - Not just for experimental research uses, but also for practical uses like sending email, browsing Internet, and so on
- When a network is designed, the purpose of network infrastructure has to be clarified
  - At the beginning stage, questions like what to achieve, how to accomplish should be identified
- Traffic flow analysis needs to be analyzed
  - Collecting data through experimental tests are essential
- Short-term investment or long-term design
  - Lifetime of ICT devices is very short, need to be updated

Planning

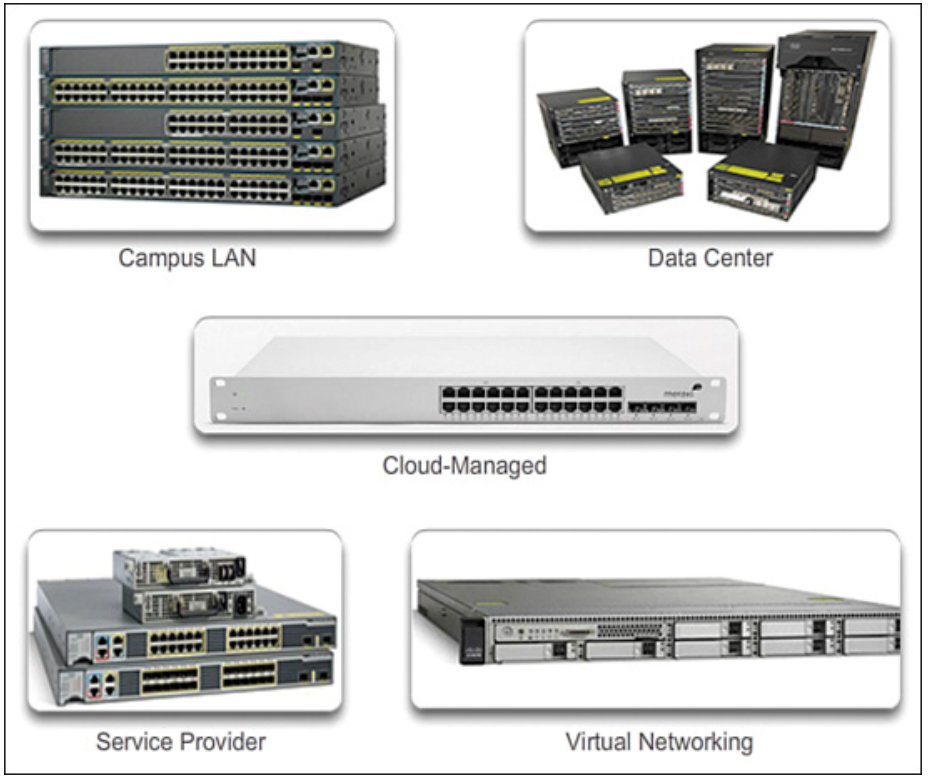
- Concept
  - More than one choices should be made on “cutting-edge”, “smart”, “stable operation” and so on
- Target
  - What are the traffic type will flow in the network?
  - Data transfer, transaction, real-time or not-real-time, one-way or two-way data transmission
- Arrangement requirements
  - New applications and services
  - Failure of the network

Analysis

- Traffic analysis
  - Analyze each type of traffic; voice, audio, data
- Topology
  - Topology of the entire networked routers and terminals
- Communication Technology
  - 10 Gigabit Ethernet, Fast Ethernet, WLAN, MPLS, etc
  - Physical medium: wireless, fiber optic, or cable
  - VLAN?
- Bandwidth need
  - Evaluation of various traffic types and determined the traffic capacity need
- Network configuration setup
  - Breakdown the details of the topology and the cable technology
- Equipment selection

Design

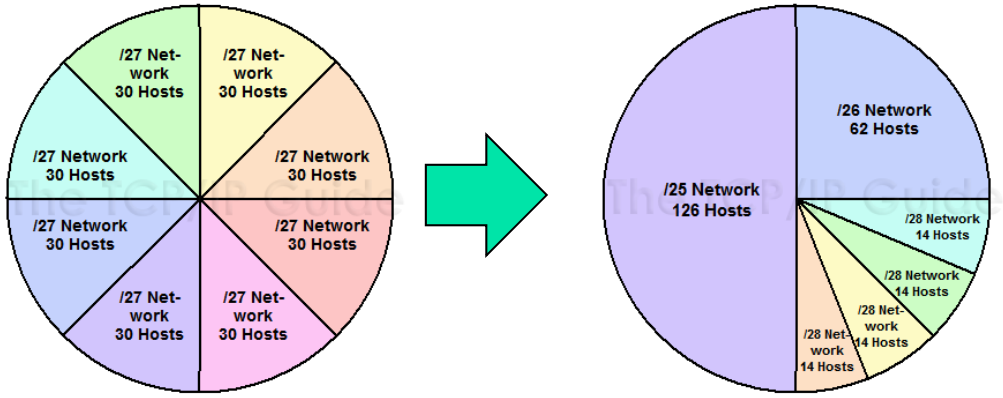
- Detailed bandwidth need
  - Confirm the total bandwidth of the traffic flow in the network
- Addressing planning and design
  - Address allocation, netmask
- Implementing design
  - Equipments, cables, heat in a server room (air conditioner) power supply design
- Parameter design
  - Bandwidth allocation with various parameter
  - Parameter settings of the selected equipments



Implementation

- Variable-length subnet mask support for the usage of any device type
  - Main weakness of conventional subnetting is that the subnet ID represents only one additional hierarchical level in how IP addresses are interpreted and used for routing – the problem with single-level subnetting
  - Variable length subnet mask (VLSM)

With traditional subnetting, all subnets must be the same size, which creates problems when there are some subnets that are much larger than others



Using VLSM, an organization can divide its IP network multiple times, to create subnets that much better match the size requirements of its physical networks

  - Dynamic routing is performed by OSPF and RIPv2
  - Router selects a route based on the longest-prefix-match algorithm

- Entry aggregation technique is used to reduce the size of routing table
  - CIDR (classless interdomain routing)

* Please see the same CIDR, Chapter 4, no. 30

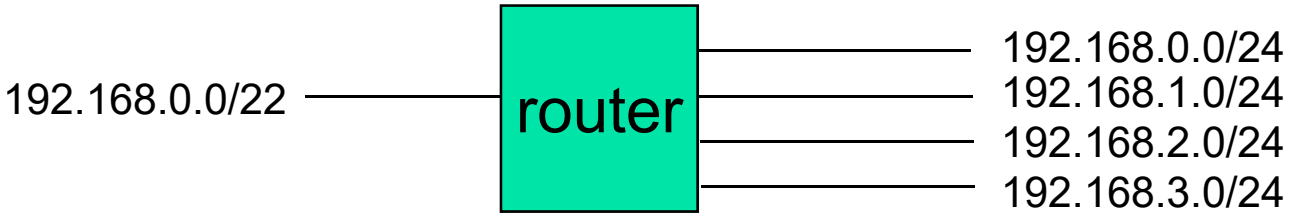
Entry Aggregation Technique (1)

192.168.0.0	1100 0000.1010 1000.0000 0000 0000 0000
192.168.1.0	1100 0000.1010 1000.0000 0001 0000 0000
192.168.2.0	1100 0000.1010 1000.0000 0010 0000 0000
192.168.3.0	1100 0000.1010 1000.0000 0011 0000 0000

Aggregated subnet mask length

Original subnet mask length

192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24
are aggregated to
192.168.0.0/22



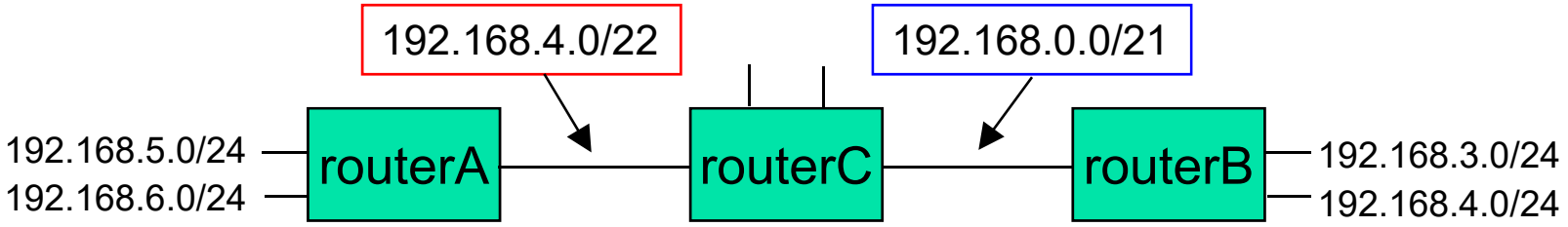
Entry Aggregation Technique (2)

192.168.3.0	1100 0000.1010 1000.0000 0011.0000 0000
192.168.4.0	1100 0000.1010 1000.0000 0100.0000 0000

192.168.5.0	1100 0000.1010 1000.0000 0101.0000 0000
192.168.6.0	1100 0000.1010 1000.0000 0110.0000 0000

192.168.0.0/21 is aggregated for router B,
meanwhile 192.168.4.0/22 is aggregated for router A

Problem!
When the longest-prefix-match is taken, router C will route the packets destined for 192.168.4.0 to router A



Bandwidth Planning

- Sum of (one-way) traffic in accordance with the link
- Bandwidth allocation is based on the total capacity at the peak hours
- If the bandwidth of a telephone line is planned, Erlang B for the required blocking probability should be considered (see Chapter 10)
  - VoP (Voice over Packet) like VoA, VoF, VoIP
  - Handling the voice traffic has to be careful
  - Through variable bit rate (VBR), the blocking probability index with different requirements should be achieved
- Response time of the application exchanging
- It is difficult to plan for a bandwidth for a network that is unpredictable behavior
  - Detail planning on ATM technology for WAN (LAN as well)
  - Threshold of the data transmission rate for LAN

Bandwidth vs. Response Time

- Consider a queue from a network equipment to a WAN, i.e., a service delivery from the network equipment to the WAN
- Below a certain response time for the service, how much needed to pay for the required bandwidth?
- Service uses a fixed packet length, called ***P*** [bit]
- Average input traffic of the service to the hardware of the network equipment is ***I*** [bit/sec]
- Required bandwidth is ***B*** [bit/sec] $\boxed{B = I/\rho}$ where channel utilization, ρ
- For M/M/1 model, mean sojourn time that is the amount of time a packet is expected to spend in a network equipment before transmitting out is given by

$$E(t_q) = E(t_w) + E(t_s) = \frac{1}{1-\rho} E(t_s) = \frac{1}{1-\rho} \frac{P}{B} = \frac{1}{1-\rho} \frac{P}{I/\rho} = \frac{\rho}{1-\rho} \frac{P}{I}$$

Average queuing time

Average service time (processing time)
Average waiting time
} Mean sojourn time

Bandwidth vs. Response Time (cont.)

How to know the required bandwidth? How to know the ρ satisfy the response time?

$$E(t_q) = \frac{\rho}{1-\rho}\frac{P}{I}$$

We known P

We can measure $E(t_q), I$

$\Rightarrow \rho \Rightarrow B$ Required bandwidth

t_q Response time

- Here the channel utilization, ρ is unknown
- To compute the channel utilization to satisfy the response time, the required bandwidth should be calculated first
- However, the mean processing time never (seldom) more than the mean sojourn time of the network equipment
- In M/M/1, let say that the sojourn time is within $\ln 10 E(t_q) \approx 2.3 E(t_q)$

  This mean that it is less than 90%
- In other words, if you want to specify the response time within a probability of 90%, we require the sojourn time is 1/2.3 (0.43) times the mean sojourn time

Numerical Example:
For B = 1 Gbps and P = 1000 bytes, I = 0.9 Gbps for 90% channel utilization resulting response time is 0.43 x 80 μs = 34.4 μs

Reliability

- Plan for disaster free or avoiding the catastrophe
  - Manually creating an alternative route in a router when the disaster happened, For example, the previous settings of network equipment are diverted
  - Configured to reduce a MTTR (mean time to repair)
- Plan for non-stop service
  - At the PHY and MAC layers, avoiding failure of equipment capabilities
  - Fast recovery proprietary
  - Depending on the multiple switches, Trunking VLAN is configured for different ports
  - Combination of High Availability (HA) server. Especially, the network connection of the outlet of a server
- Training
  - When network down, user failed to use will spread
  - What problem exist? How to train to user?

Technology Improving Reliability

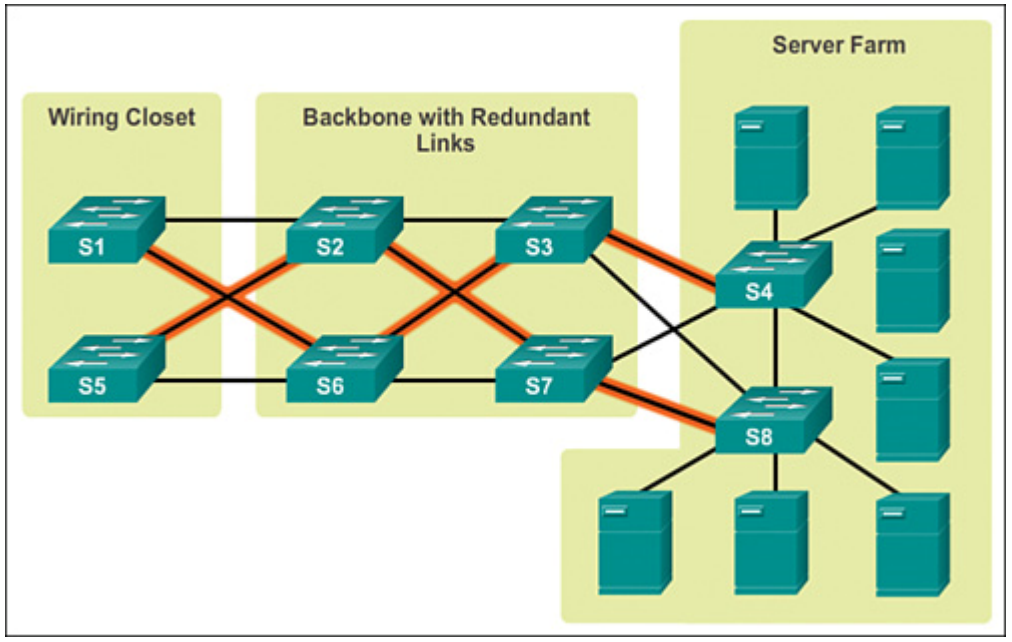
- Use of dynamic routing, the default routing
- Through heartbeat examination, router is switched to standby mode
  - Switching router protocol (RFC2338 VRRP = Virtual Router Redundancy Protocol, and other proprietary protocols)
  - HA server (cluster)
- Ring connection route (connected triangles)
  - Spanning Tree (802.1D STP = shielded twisted pair, 801.1W Fast STP, and other proprietary protocols)
  - Dual Ring
  - Dual port NIC (network interface card)

Implementation

- Cabling
  - Line maneuverability (skillful management), curvature (twisting), labeling
- Equipment installation and configuration
  - Setting
  - Labeling
- Unit testing equipment
  - Equipment operation check
  - Link status
  - Operational temperature (20-21 degree Celsius for a server room)

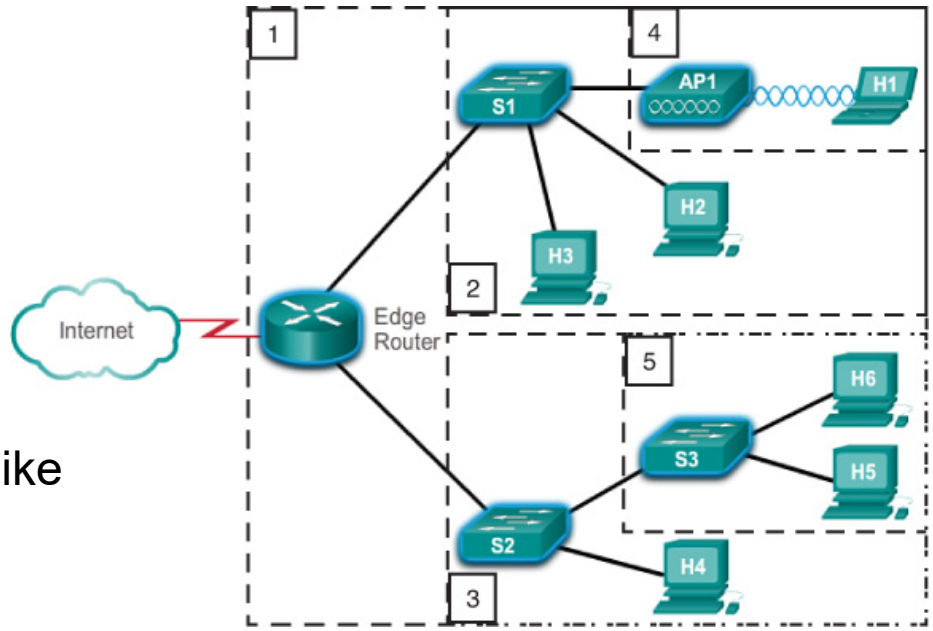
Network Testing

- Making test up to the network layer
- Communication test
  - ping
  - Path validation
- Traffic load test
  - Increase channel utilization
  - Tester traffic generator
  - File transfer
- Backup test
  - Disconnect the cable
  - Stop the equipment



Entire Testing

- Application-level test
- Server and client interaction
- Communication test
  - Various packet sizes and traffic pattern
- Performance evaluation
  - Application-level performance, like latency
  - Load balancing mechanism
- Including the backup server to be tested
  - Server backup feature
  - Operation test, including HA (high availability) server



Migration

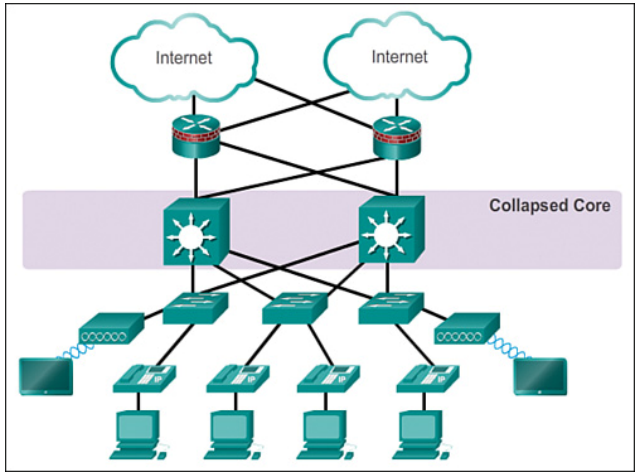
- Changing network
  - Examination of coexistence
  - Consistency with the end-user applications
  - Operational timing: Balance between business hours
  - Announcement, training

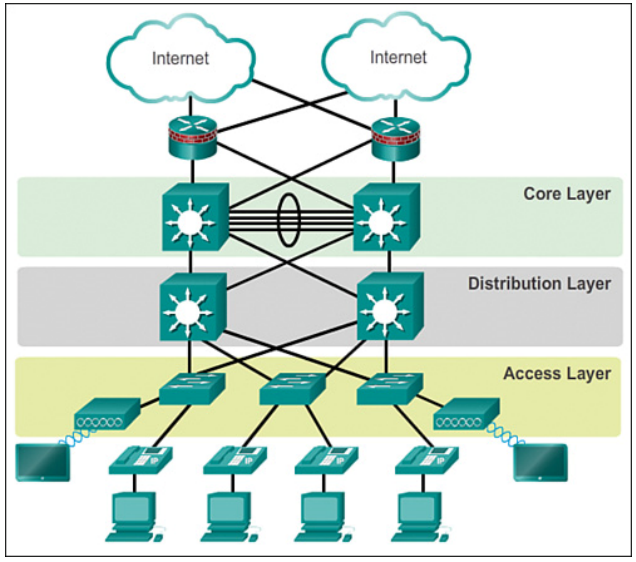
Maintenance, Management, Operation

- Traffic monitoring
  - Understanding of normal operation
  - Trend of data analysis
- Resource management
  - Maintenance Information
  - Centralized configuration management
  - Documentation
- Accumulation of information failure
  - Model-dependent information failure
  - Operation-dependent information failure

LAN Routing Architecture

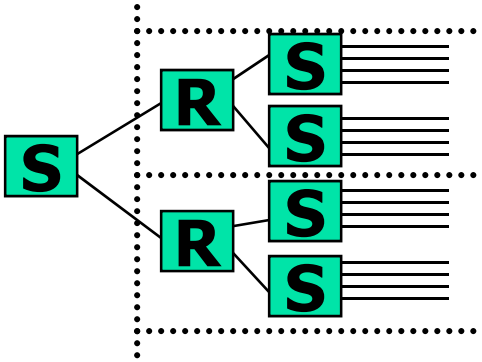
- How do I place a (function) network equipment?
- Core and edge
  - User device has a dedicated line to edge
  - Edges are connected to core
- Location of routing function
  - At the L3 layer or at the L2 layer
  - 80:20 rule interpretation. It means that the percentages of traffic to local and traffic to backbone
  - Traffic pattern. Traffic to the shared resources, local traffic, traffic between edge nodes
- Aggregation router / switch
  - Placed it in the middle to get the beneficial of aggregation



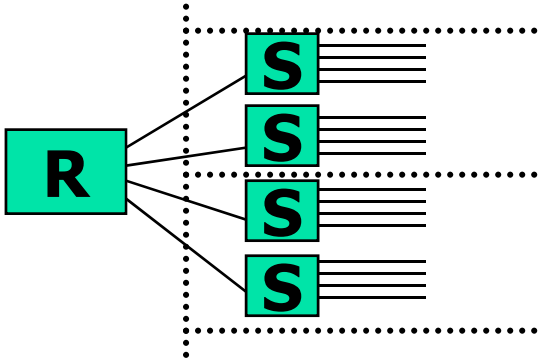


Distributed and centralized of a Router

- L2 switch in between distributed routers
  - Edge-oriented router
  - Traffic pattern in between the edge nodes
  - Increases the number of routers
  - Reliability and load balancing
  - The increase in administrative burden
  - Partial upgrade is possible



- Extending connection in between the collapsed backbone and edge routers
  - Routing at the center, edge is only L2 switch
  - Resource is placed at the center, everyone has access to it
  - Router is a single or a few
  - Reliability and the required load is concentrated
  - Management is less
  - Upgrade of the entire system can be in one place
  - Increase the line from router to edge



What is Network Management?

Basic tasks that fall under this category are:

- Configuration Management
  - Keeping track of device settings and how they function
- Fault Management
  - Dealing with problems and emergencies in the network (router stops routing, server loses power, etc)
- Performance Management
  - How smoothly is the network running?
  - Can it handle the workload it currently has?
- The management interface must be
  - Standardized, extendible, portable
- The management mechanism must be
  - Inexpensive, implemented as software only

Network Management Protocol

Two management models:

- OSI specified network management model
  - E.g., CMIP (common management information protocol)
  - CMIP allows both modification and performing actions on managed objects
  - CMIP provides good security
  - For managing devices on telecommunication networks
- IETF specified network management model
  - E.g., SNMP (simple network management protocol)
  - Simple and minimum functionalities
  - For managing devices on IP networks
- On the Internet, most TCP/IP devices support SNMP and not CMIP. This is because of the complexity and resource requirements of CMIP agents and management systems.

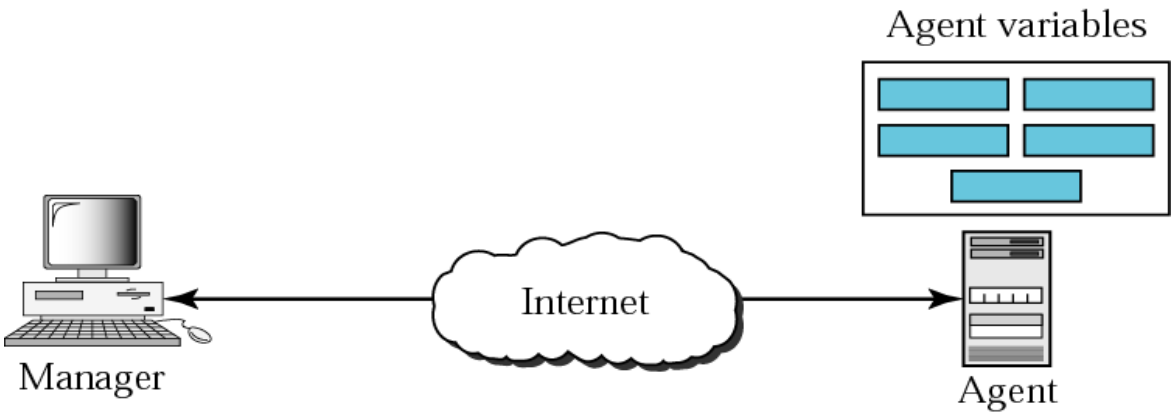
SNMP & Network Management History

- *1983* TCP/IP replaces ARPANET at U.S. Dept. of Defense, effective birth of Internet
- *Oct 1987* First model for network management, HEMS – High-level Entity Management System (*RFCs 1021,1022,1024,1076*), but it not use for the Internet
- *Nov 1987* SGMP – Simple Gateway Monitoring protocol (*RFC 1028*)
- *1987* ISO OSI proposes CMIP and CMOT (CMIP over TCP) for the actual network management protocol for use on the Internet, but failed
- *1989* Marshall T. Rose heads up SNMP working group to create a common network management framework to be used by both SGMP and CMOT
- *Apr 1989* SNMP promoted to *recommended* status as the de facto TCP/IP network management framework (*RFC 1098*)
- *Jun 1989* Internet Activity Boards (IAB) committee decides to let SNMP and CMOT develop separately
- *Aug 1989* "Internet-standard Network Management Framework" defined (*RFCs 1065, 1066, 1067*)
- *May 1990* IAB promotes SNMP to a standard protocol with a recommended status (*RFC 1157*)
- *Mar 1991* Format of MIBs and traps defined (*RFCs 1212, 1215*)
- TCP/IP MIB definition revised to create SNMPv1 (RFC 1213)

* RFC denotes Request for Comments

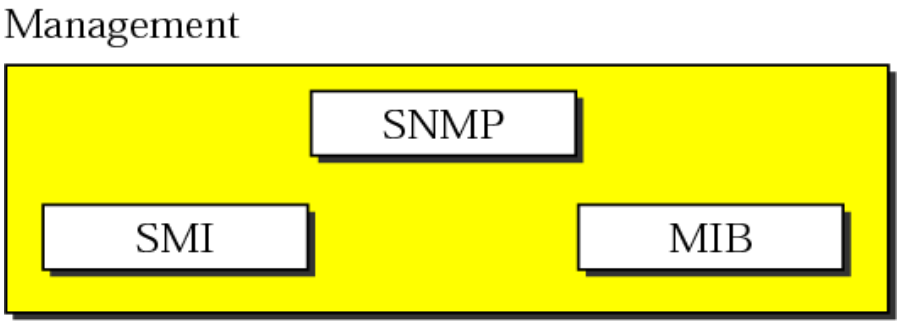
What is SNMP?

- SNMP is a tool (protocol) that allows for remote and local management of items on the network including servers, workstations, routers, switches and other managed devices
- Comprised of agents and managers:
  - Agent - process running on each managed node collecting information about the device it is running on
  - Manager - process running on a management workstation that requests information about devices on the network



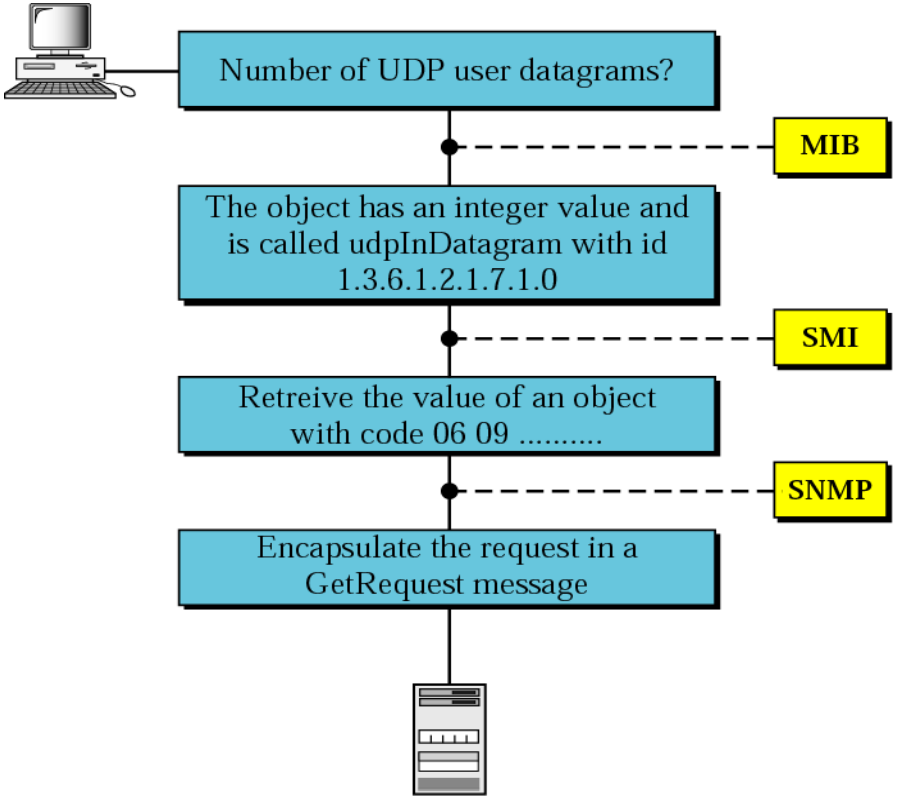
More About SNMP

- SNMP is a "client pull" model
  - Management system (client) "pulls" data from the agent (server)
- SNMP is a "server push" model
  - Agent (server) "pushes" out a trap message to a (client) management system
- SNMP requires the use of two other protocols:
  - Structure of management information (SMI), and
  - Management information base (MIB)
- Network management on the Internet is done through the cooperation of SNMP, SMI, and MIB



Three Parts of SNMP

- SNMP
  - Defines format of messages exchanged by management systems and agents
  - Specifies the Get, GetNext, Set, and Trap operations
- SMI
  - Rules specifying the format used to define objects managed on the network that the SNMP protocol accesses
- MIB
  - A map of the hierarchical order of all managed objects and how they are accessed



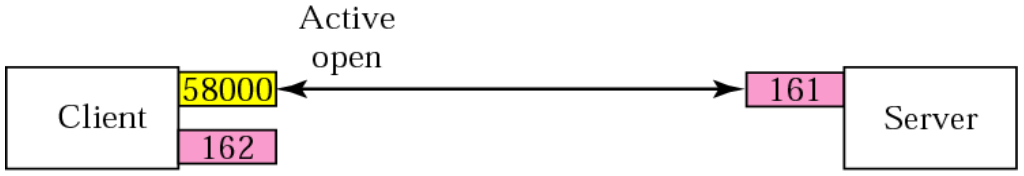
The OSI Model & SNMP

7	Application Layer	Management and Agent APIs SNMP
6	Presentation Layer	ASN.1 and BER
5	Session Layer	RPC and NetBIOS
4	Transport Layer	TCP and UDP
3	Network Layer	IP and IPX
2	Data Link Layer	Ethernet, Token Ring, FDDI
1	Physical Layer	

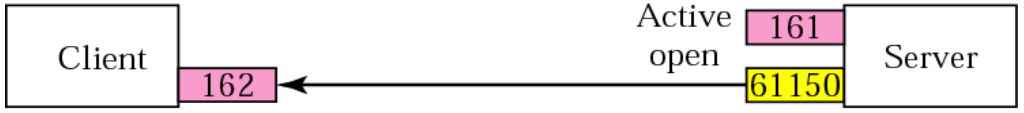
Ports & UDP

- SNMP uses UDP as the transport mechanism for SNMP messages
- Like FTP, SNMP uses two well-known ports to operate
  - UDP Port 161 - SNMP Messages
  - UDP Port 162 - SNMP Trap Messages

a. Passive open by both client and server



b. Exchange of request and response messages



c. Server sends trap message

SNMP Agents

- Extendible Agents
  - Open, modular design allows for adaptations to new management data and operational requirements
- Monolithic Agents
  - Not extendible
  - Optimized for specific hardware platform and OS
  - This optimization results in less overhead (memory and system resources) and quicker execution
- Proxy & Gateway Agents
  - Manage a device that cannot support an SNMP agent
  - Manage a device that supports a non-SNMP management agent
  - Allow a non-SNMP management system to access an SNMP agent
  - Provide firewall-type security to other SNMP agents (UDP packet filtering)
  - Translate between different formats of SNMP messages (v1 and v2)
  - Consolidate multiple managed nodes into a single network address (also to provide a single trap destination)

Four Basic Operations

- `Get`
  - Retrieves the value of a MIB variable stored on the agent machine (integer, string, or address of another MIB variable)
- `GetNext`
  - Retrieves the next value of the next lexical MIB variable
- `Set`
  - Changes the value of a MIB variable
- `Trap`
  - Unsolicited notification sent by an agent to a management application (typically a notification of something unexpected, like an error)

Traps

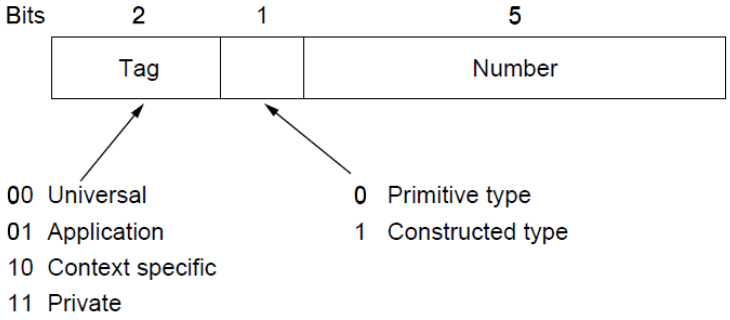
- Traps are unrequested event reports that are sent to a management system by an SNMP agent process
- When a trappable event occurs, a trap message is generated by the agent and is sent to a trap destination (a specific, configured network address)
- Many events can be configured to signal a trap, like a network cable fault, failing NIC or Hard Drive, a “General Protection Fault”, or a power supply failure
- Traps can also be throttled – limit the no. of traps sent per second from the agent
- Traps have a priority associated with them – Critical, Major, Minor, Warning, Marginal, Informational, Normal, Unknown
- Traps are received by a management application, which can handle the trap in a few ways
  - Poll the agent that sent the trap for more information about the event, and the status of the rest of the machine
  - Log the reception of the trap
  - Completely ignore the trap

Languages of SNMP

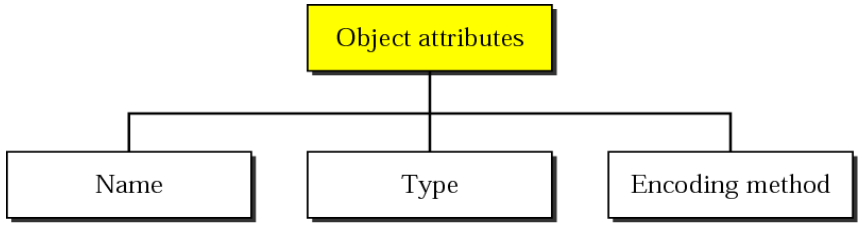
- Structure of management information (SMI)
  - SMI is a component used in network management
  - Specifies the format used for defining managed objects that are accessed via the SNMP protocol
- Abstract syntax notation one (ASN.1)
  - Used to define the format of SNMP messages and managed objects (MIB modules) using an unambiguous data description format
- Basic encoding rules (BER)
  - Used to encode the SNMP messages into a format suitable for transmission across a network

SMI

- SMI names objects, defines the data type that can be stored in an object, and shows how data can be encoded over the network
- Name
  - All objects managed by SNMP are given an object identifier
- Data type
- Encoding method



The first byte of each data item sent in the ASN.1 transfer syntax



Data Type	*Class*	*Format*	*Number*	*Tag (Binary)*	*Tag (Hex)*
INTEGER	00	0	00010	**00000010**	**02**
OCTET STRING	00	0	00100	**00000100**	**04**
OBJECT IDENTIFIER	00	0	00110	**00000110**	**06**
NULL	00	0	00101	**00000101**	**05**
Sequence, sequence of	00	1	10000	**00110000**	**30**
IPAddress	01	0	00000	**01000000**	**40**
Counter	01	0	00001	**01000001**	**41**
Gauge	01	0	00010	**01000010**	**42**
TimeTicks	01	0	00011	**01000011**	**43**
Opaque	01	0	00100	**01000100**	**44**

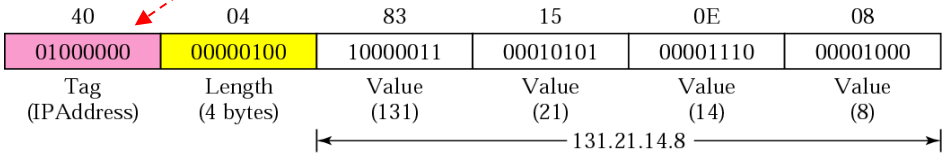


Figure: Example of IP address 131.21.14.8

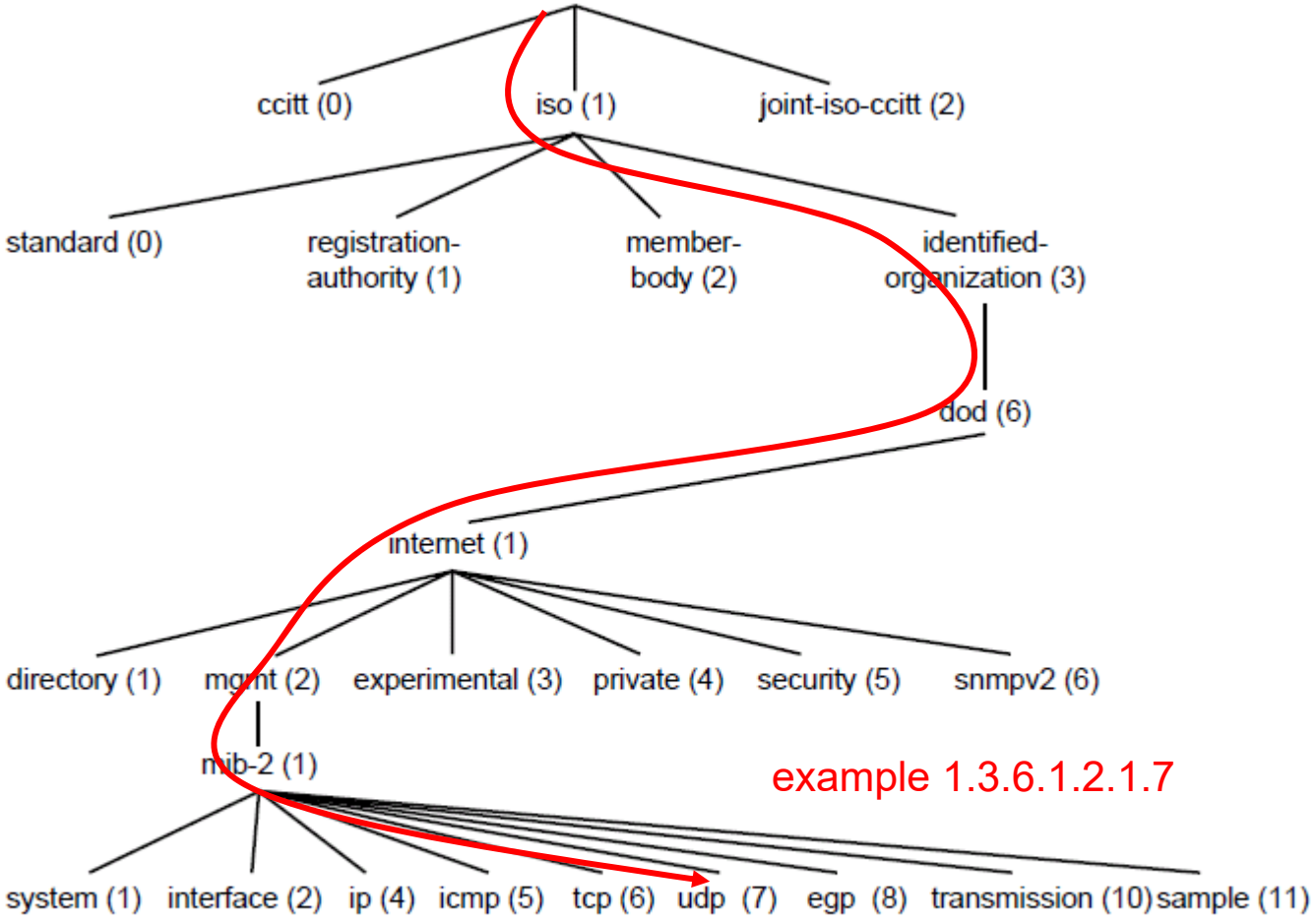
ASN.1

- ASN.1 is a formal language for describing data and the properties of the data. It says nothing about how the data is stored or encoded
- It is similar to C/C++ and other programming languages
- All the fields in the MIB and the SNMP messages are described in ASN.1. For syntax examples, ASN.1 of data type `IpAddress` from the SMI looks like:

```
IpAddress ::=
    [APPLICATION 0]                 # in network-byte order
        IMPLICIT OCTET STRING (SIZE (4))
```

- From MIB we find the following definition of a simple variable:

```
udpNoPorts OBJECT-TYPE
    SYNTAX          Counter
    ACCESS          read-only
    STATUS          mandatory
    DESCRIPTION     "The total number of received UDP datagrams for which there was no
                     application at the destination port."
    ::= { udp 2 }
```



Part of the ASN.1 object naming tree

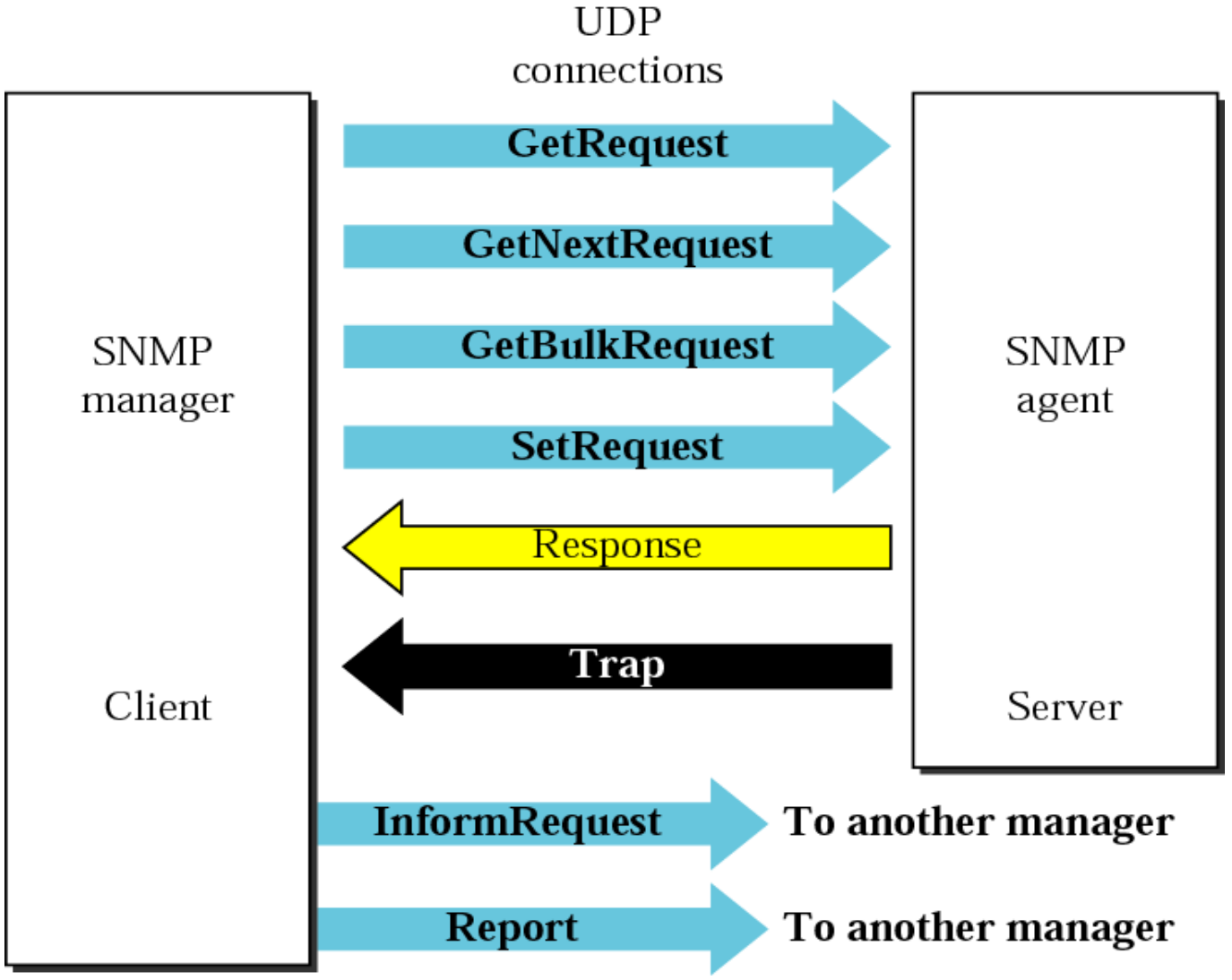
BER

- Given the ASN.1 definition, there are many ways to encode the data into a stream of bits for transmission. SNMP uses BER
- All SNMP messages are converted / serialized from ASN.1 notation into smaller, binary data (BER)
- The relationship between ASN.1 and BER parallels that of source code and machine code
- ITU X.209 specifies the BER for ASN.1. X.209 has been withdrawn on 30 Oct. 2002 and has been superseded by X.690

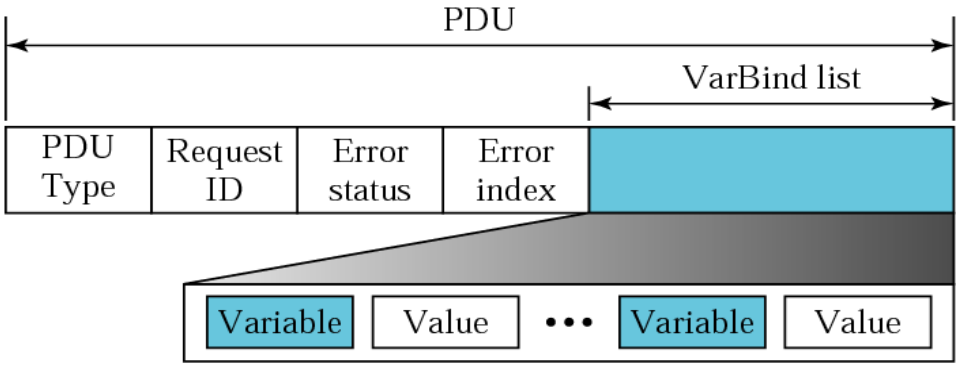
SNMP Data Type

Type	*Size*	*Description*
INTEGER	4 bytes	An integer with a value between -2^{31} and $2^{31}-1$
Integer32	4 bytes	Same as INTEGER
Unsigned32	4 bytes	Unsigned with a value between 0 and $2^{32}-1$
OCTET STRING	Variable	Byte-string up to 65,535 bytes long
OBJECT IDENTIFIER	Variable	An object identifier
IPAddress	4 bytes	An IP address made of four integers
Counter32	4 bytes	An integer whose value can be incremented from zero to 2^{32}; when it reaches its maximum value it wraps back to zero
Counter64	8 bytes	64-bit counter
Gauge32	4 bytes	Same as Counter32, but when it reaches its maximum value, it does not wrap; it remains there until it is reset
TimeTicks	4 bytes	A counting value that records time in 1/100ths of a second
BITS		A string of bits
Opaque	Variable	Uninterpreted string

SNMP PDU Connection



SNMP PDU Format



Differences:

1. Error status and error index values are zeros for all request messages except GetBulkRequest.
2. Error status field is replaced by non-repeater field and error index field is replaced by max-repetitions field in GetBulkRequest.

Status	*Name*	*Meaning*
0	noError	No error
1	tooBig	Response too big to fit in one message
2	noSuchName	Variable does not exist
3	badValue	The value to be stored is invalid
4	readOnly	The value cannot be modified
5	genErr	Other errors

Table: Types of errors

SNMP Message

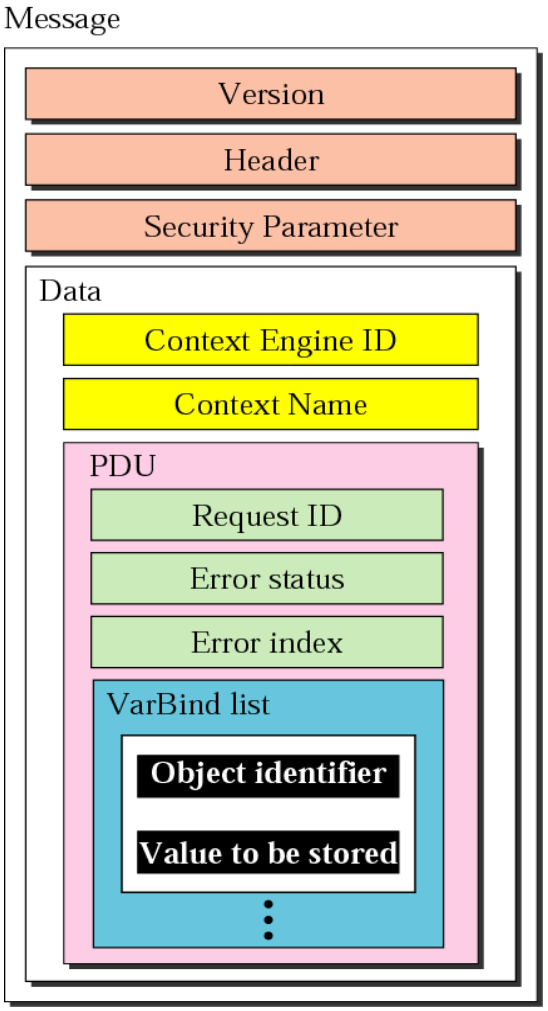
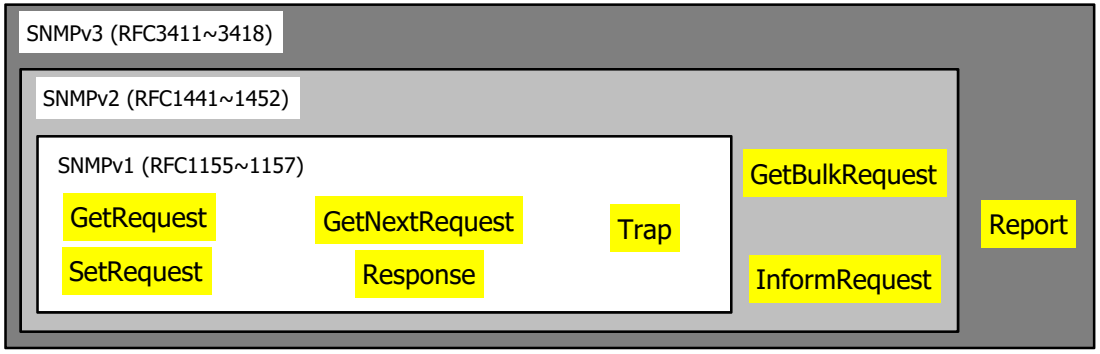


Figure: SNMP message

Data	*Class*	*Format*	*Number*	*Whole Tag (Binary)*	*Whole Tag (Hex)*
GetRequest	10	1	00000	**10100000**	**A0**
GetNextRequest	10	1	00001	**10100001**	**A1**
Response	10	1	00010	**10100010**	**A2**
SetRequest	10	1	00011	**10100011**	**A3**
GetBulkRequest	10	1	00101	**10100101**	**A5**
InformRequest	10	1	00110	**10100110**	**A6**
Trap (SNMPv2)	10	1	00111	**10100111**	**A7**
Report	10	1	01000	**10101000**	**A8**

Table: Codes for SNMP messages



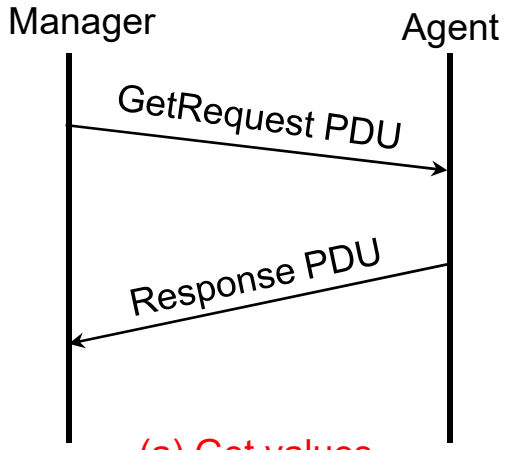
Transmission of SNMP Message

- PDU is constructed using **ASN.1**
- PDU is passed to an **authentication** service with a community name and source & destination transport addresses passed
  - Authentication service performs any required transformations such as encryption or the inclusion of an authentication code
- Protocol entity then constructs a message, consisting of a **version field**, the **community name**, and the **result from step 2**
- This new ASN.1 object is then encoded using **BER** and passed to the transport service

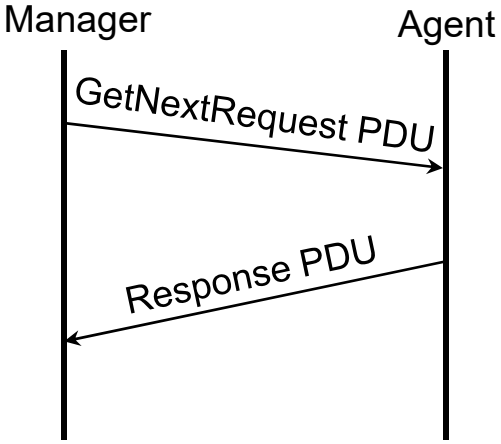
Receipt of SNMP Message

- SNMP entity performs basic syntax-check of the message and discards it if it fails to parse
- It also verifies the version number and discards it if there is a mismatch
- It then passes the community name, the PDU portion of the message and the source/destination transport address to an authentication service
  - If authentication fails, the message is discarded
  - If authentication succeeds, the authentication service returns a PDU in the form of an ASN.1 object
- If the PDU passes the basic syntax-check, the appropriate SNMP access policy is selected and the PDU is processed accordingly

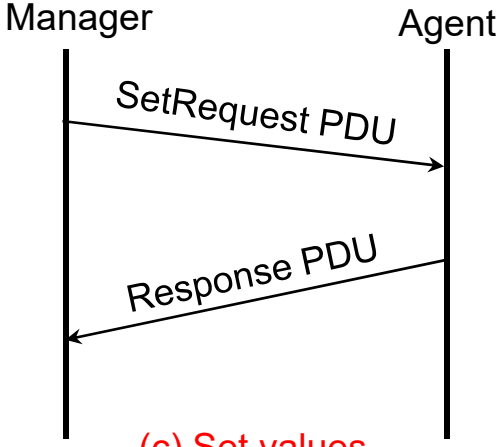
SNMP PDU Sequences



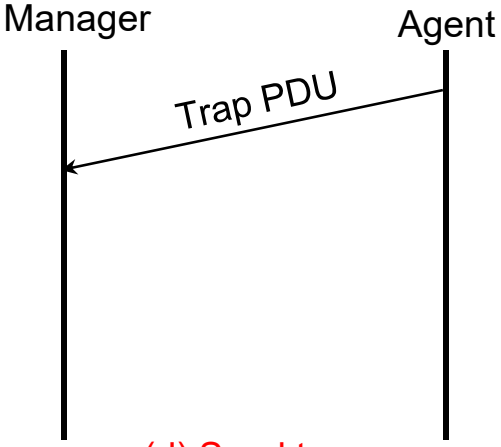
(a) Get values



(b) Get next values



(c) Set values



(d) Send trap

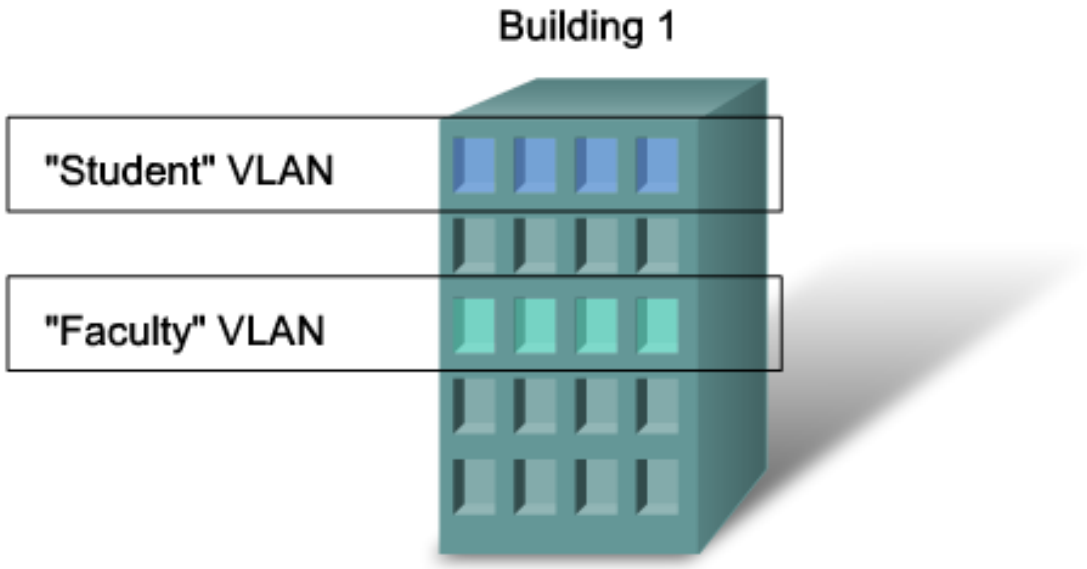
Limitations and Status of SNMP

- SNMPv1 is not well suited for retrieving large volumes of data, such as an entire routing table
- SNMPv1 MIB model is limited (does not support management queries based on object types or values)
- SNMPv1 traps are unacknowledged & may not be delivered
- SNMPv1 provides only trivial authentication
- SNMPv1 does not support explicit actions & manager-to-manager (M2M) communications
- SNMPv2
  - Improvements in the areas of performance, security, confidentiality, and M2M communications
  - Overly complex and it was not widely accepted
- SNMPv3 added security and remote configuration enhancements

Virtual LANs (VLANs)

- VLAN allows a network administrator to create groups of logically networked devices that act as if they are on their own independent network, even if they share a common infrastructure with other VLANs
- Using VLANs, you can logically segment switched networks based on functions, departments, or project teams
- You can also use a VLAN to geographically structure your network to support the growing reliance of companies on home-based workers
- These VLANs allow the network administrator to implement access and security policies to particular groups of users

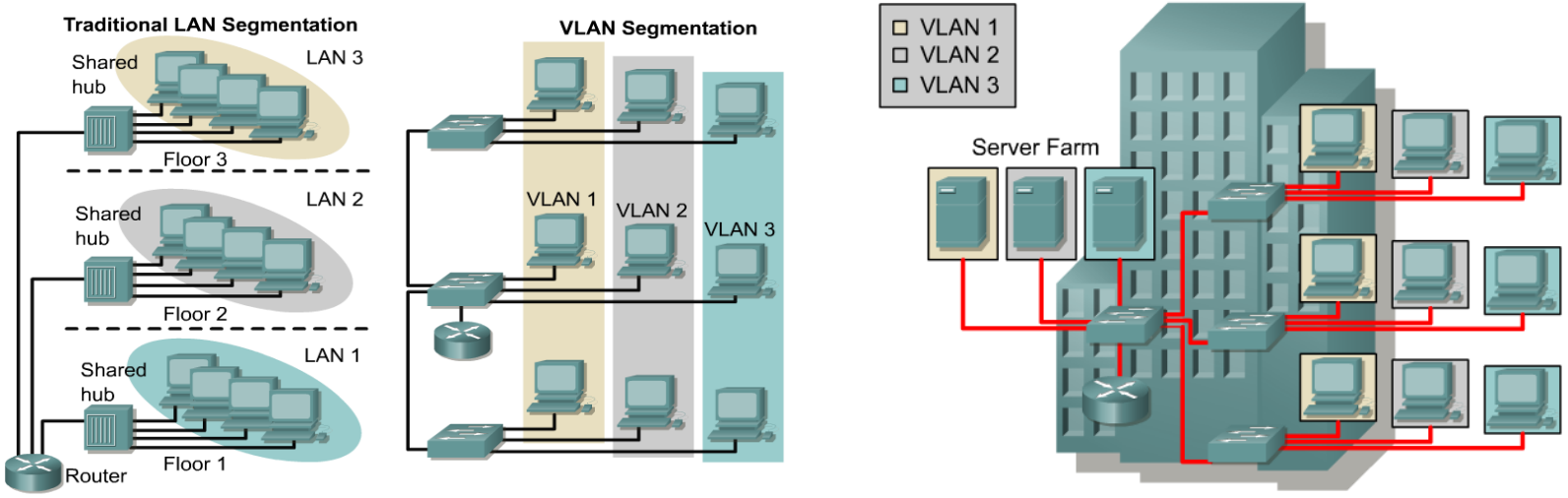
VLAN Overview



- A VLAN is an independent LAN network.
- A VLAN allows student and faculty PCs to be separated although they share the same infrastructure.
- A VLAN can be named for easier identification

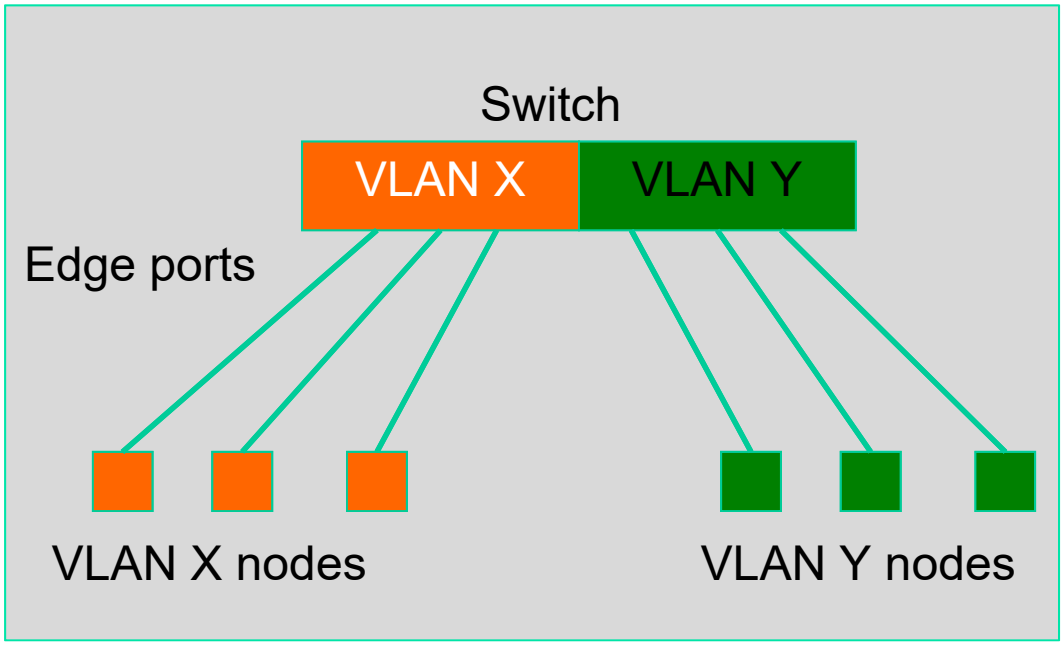
VLAN Introduction

- VLANs provide segmentation based on broadcast domains
- VLANs logically segment switched networks based on the functions, project teams, or applications regardless of the physical location or connections to the network
- All workstations and servers used by a particular workgroup share the same VLAN



Local VLAN

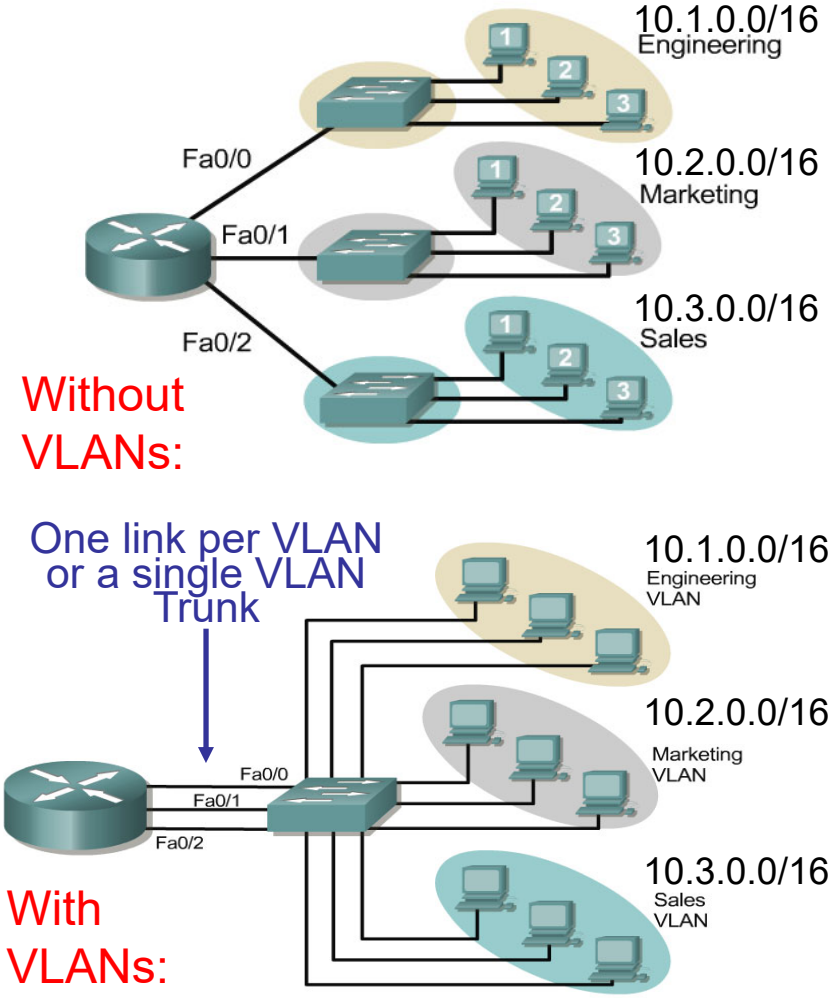
- 2 VLANs or more within a single switch
- VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management
- Edge ports, where end nodes are connected, are configured as members of a VLAN



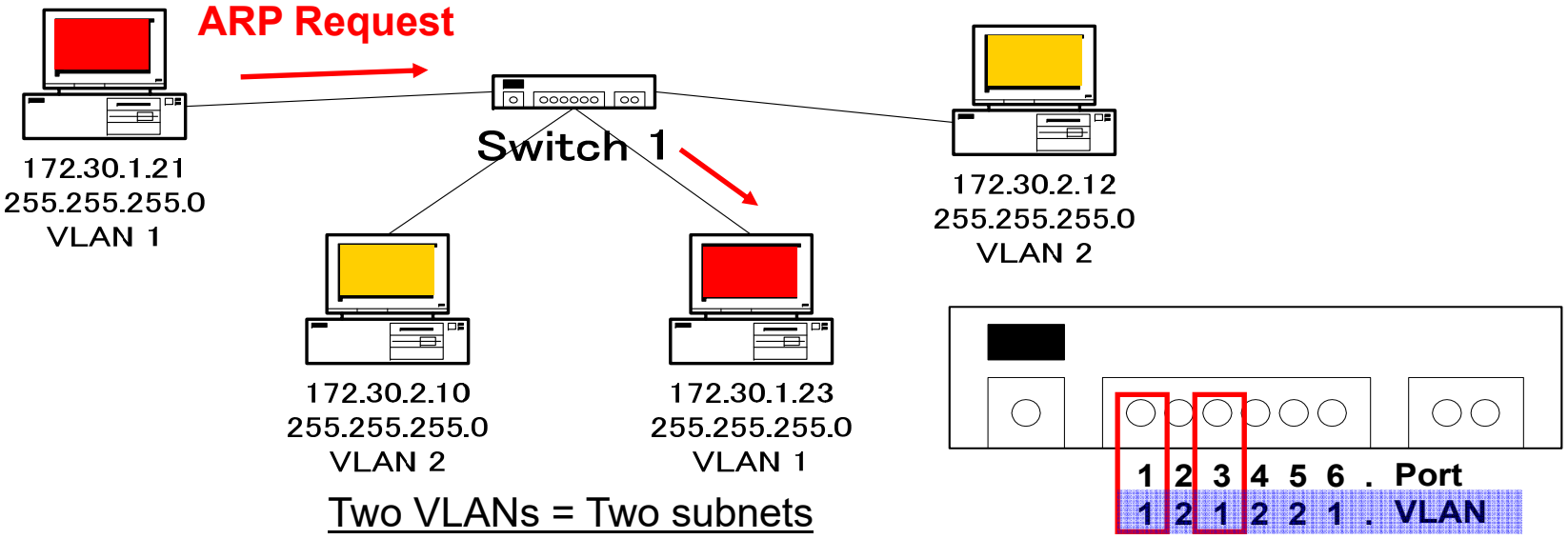
- The switch behaves as several virtual switches, sending traffic only within VLAN members
- Switches may not bridge any traffic between VLANs, as this would violate the integrity of the VLAN broadcast domain
- Traffic should only be routed between VLANs

Broadcast Domains with VLAN & Router

- Without VLANs, each group is on a different IP network and on a different switch
- Using VLANs. Switch is configured with the ports on the appropriate VLAN. Still, each group on a different IP network; however, they are all on the same switch
- What are the broadcast domains in each?



Important Notes on VLAN

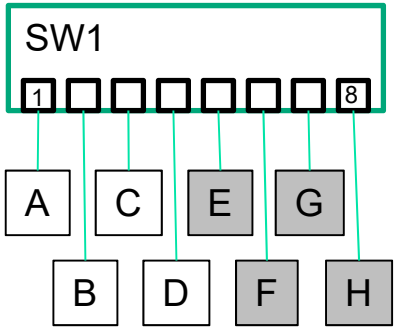


Two VLANs = Two subnets

- VLANs are assigned to switch ports only and not to a host
- Making the host to be a part of a VLAN, it must be assigned an IP address that belongs to the proper subnet, remember: VLAN = subnet
- VLANs separate broadcast domain. Without VLAN, the ARP would be seen on all subnets
- Assigning a host to the correct VLAN using a 2-step process
  1. Connect the host to the correct port on the switch
  2. Assign the host to the correct IP address based on the VLAN membership

VLAN in Ethernet

- Port grouping of Ethernet

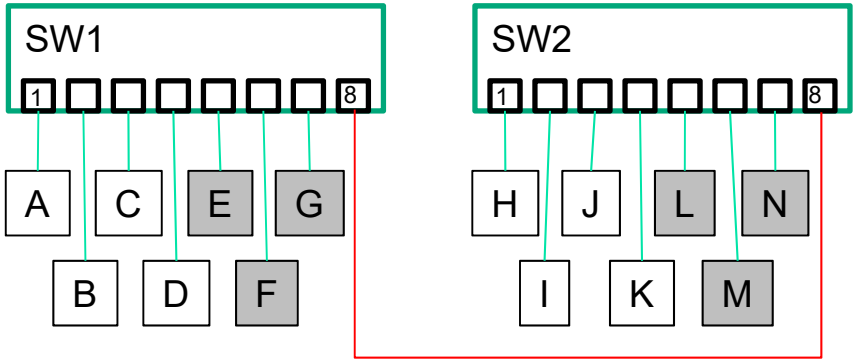


Port	MAC Address
1	A
2	B
3	C
4	D
5	E
6	F
7	G
8	H

Port	MAC Address
1	A
2	B
3	C
4	D

Port	MAC Address
5	E
6	F
7	G
8	H

- Tag for inter-switch, VID for intra-switch



SW1, SW2

VID	Untag Ports	Tag Ports
100	1, 2, 3, 4	8
101	5, 6, 7	8

SW1

VID: 100

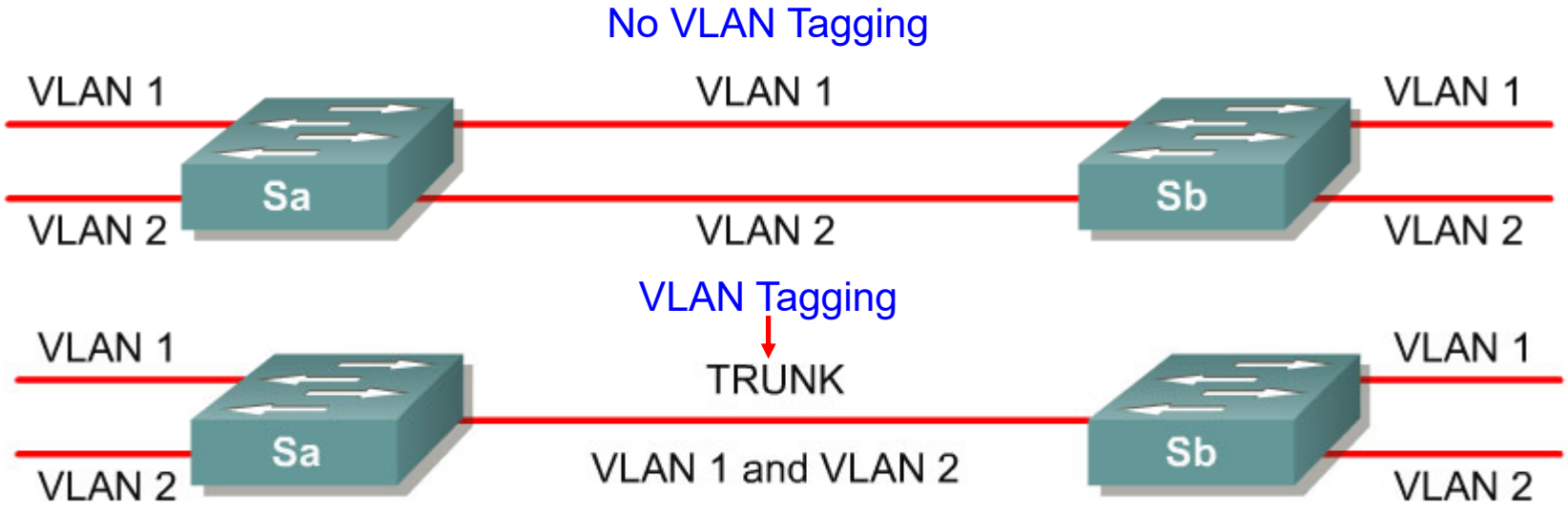
Port	MAC Address
1	A
2	B
3	C
4	D
8	H, I, J, K

VID: 101

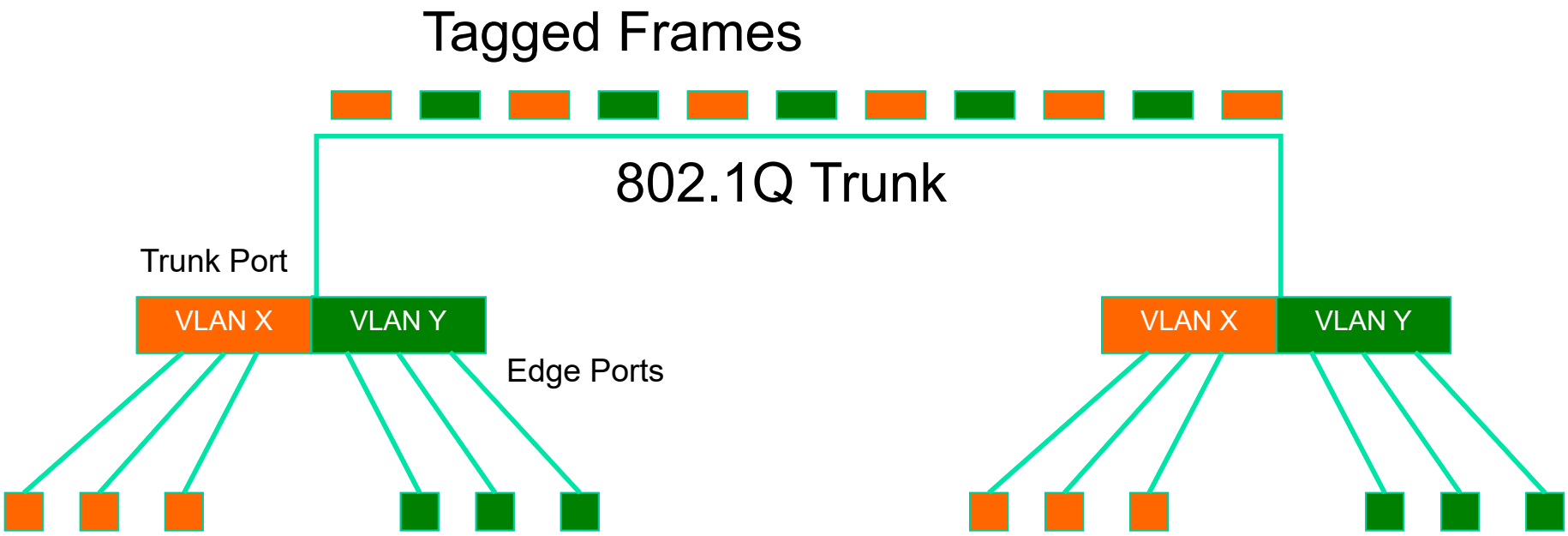
Port	MAC Address
5	E
6	F
7	G
8	L, M, N

VLAN Across Switches

- Two switches can exchange traffic from one or more VLANs
- Inter-switch links are configured as trunks, carrying frames from all or a subset of a switch's VLANs
- Each frame carries a tag that identifies which VLAN it belongs to
- VLAN tagging is used when a single link needs to carry traffic for more than one VLAN



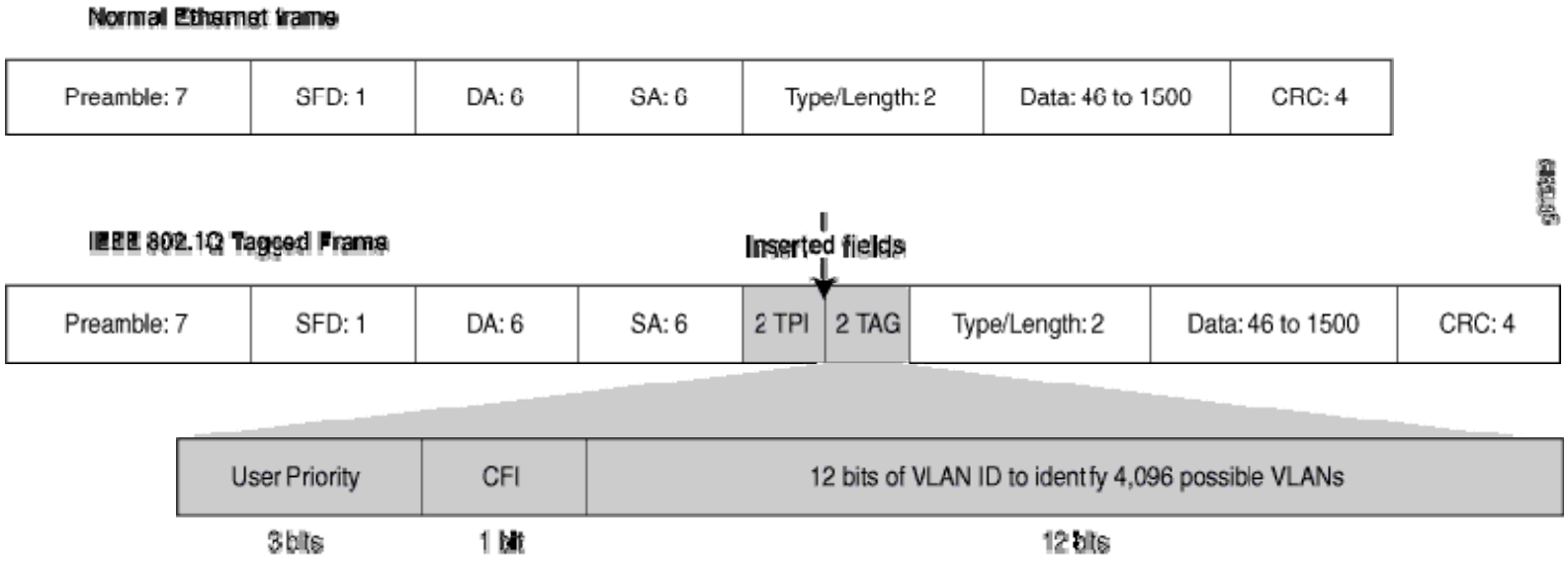
VLAN Across Switches (cont.)



This is called "VLAN Trunking"

IEEE 802.1Q

- IEEE standard that defines how Ethernet frames should be tagged when moving across switch trunks
- This means that switches from different vendors are able to exchange VLAN traffic



Tagged vs. Untagged

- Edge ports are not tagged, they are just “members” of a VLAN
- You only need to tag frames in switch-to-switch links (trunks), when transporting multiple VLANs
- Trunk can transport both tagged and untagged VLANs
  - As long as the two switches agree on how to handle those

VLAN Increase Complexity

- You can no longer “just replace” a switch
  - Now you have VLAN configuration to maintain
  - Field technicians need more skills
- You have to make sure that all the switch-to-switch trunks are carrying all the necessary VLANs
  - Need to keep in mind when adding/removing VLANs

VLAN Discussion

Advantages:

- You want to segment your network into multiple subnets, but can't buy enough switches
  - Hide sensitive infrastructure like IP phones, building controls, etc
- Separate control traffic from user traffic
  - Restrict who can access your switch management address

Disadvantages:

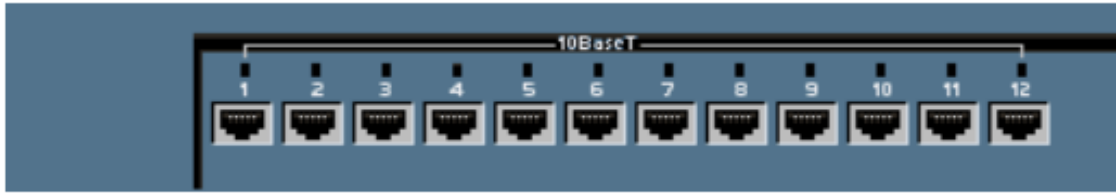
- Because you can, and you feel cool ☺
- Because they will completely secure your hosts (or so you think)
- Because they allow you to extend the same IP network over multiple separate buildings

Do Not Build "VLAN Spaghetti"

- Extending a VLAN to multiple buildings across trunk ports
- Bad idea because
  - Broadcast traffic is carried across all trunks from one end of the network to another
  - Broadcast storm can spread across the extent of the VLAN
  - Maintenance and troubleshooting nightmare

Configuring Static VLAN

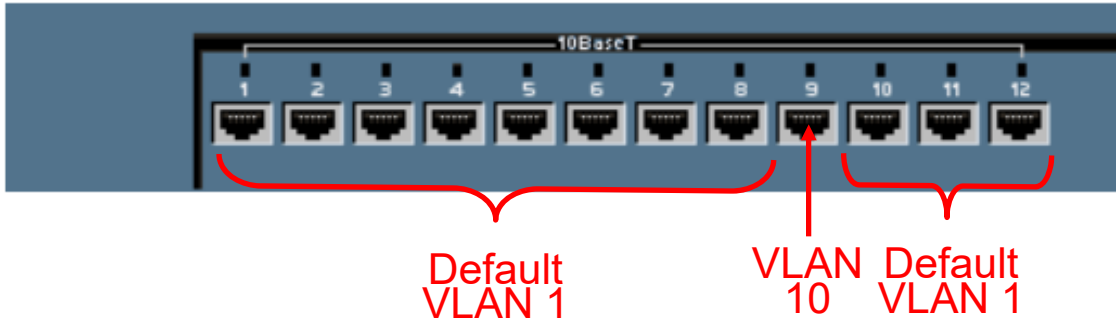
- VLAN 1 is one of the factory-default VLANs
- Configure VLANs:
  - `Switch #conf t`
  - `Switch(config) #interface vlan 10`
  - `Switch(config-if)#ip address x.x.x.x m.m.m.m`



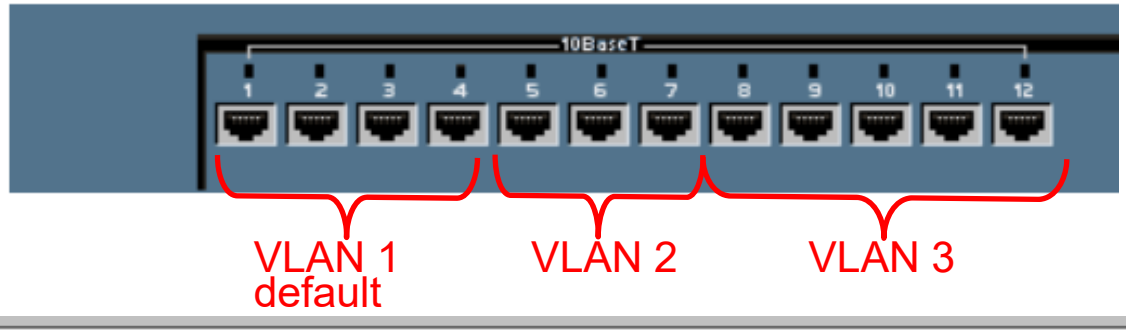
Creating VLAN

- Create the VLAN:
  - `Switch #vlan database`
  - `Switch(vlan)#vlan vlan_number`
  - `Switch(vlan)#exit`
- Assign ports to the VLAN (in configuration mode):
  - `Switch(config) #interface fastethernet 0/9`
  - `Switch(config-if)#switchport access vlan 10`

Note: access denotes this port as an access port and not a trunk



Verifying VLAN: `show vlan-switch`



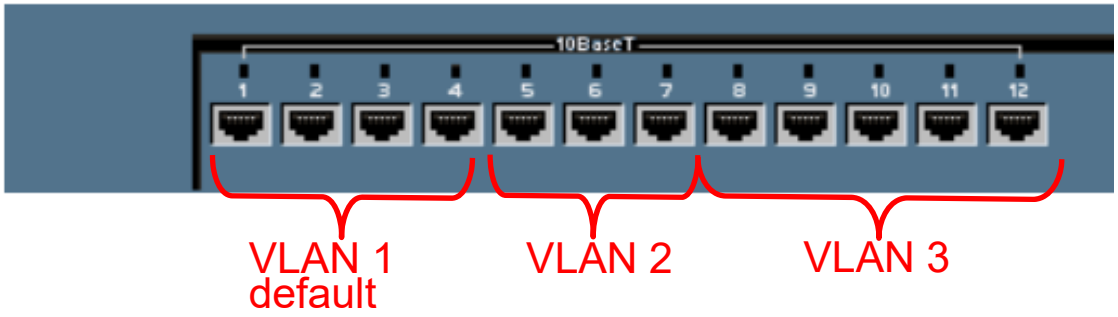

```
SydneySwitch#show vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VLAN2                            active    Fa0/5, Fa0/6, Fa0/7
3    VLAN3                            active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                                Fa0/12
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
```

Verifying VLAN: `show vlan-switch brief`




```
SydneySwitch#show vlan-switch brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VLAN2                            active    Fa0/5, Fa0/6, Fa0/7
3    VLAN3                            active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                                Fa0/12
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

VLAN Database Commands

- Optional command to add, delete, or modify VLANs
- VLAN names, numbers, and VTP (VLAN Trunking Protocol) information can be entered which “may” affect other switches
- This command does not assign any VLANs to an interface

```
Switch# vlan database
Switch(vlan)#?
VLAN database editing buffer manipulation commands:
  abort  Exit mode without applying the changes
  apply  Apply current changes and bump revision number
  exit   Apply changes, bump revision number, and exit mode
  no     Negate a command or set its defaults
  reset  Abandon current changes and reread current database
  show   Show database information
  vlan   Add, delete, or modify values associated with a single VLAN
  vtp    Perform VTP administrative functions
```

VLAN Trunking

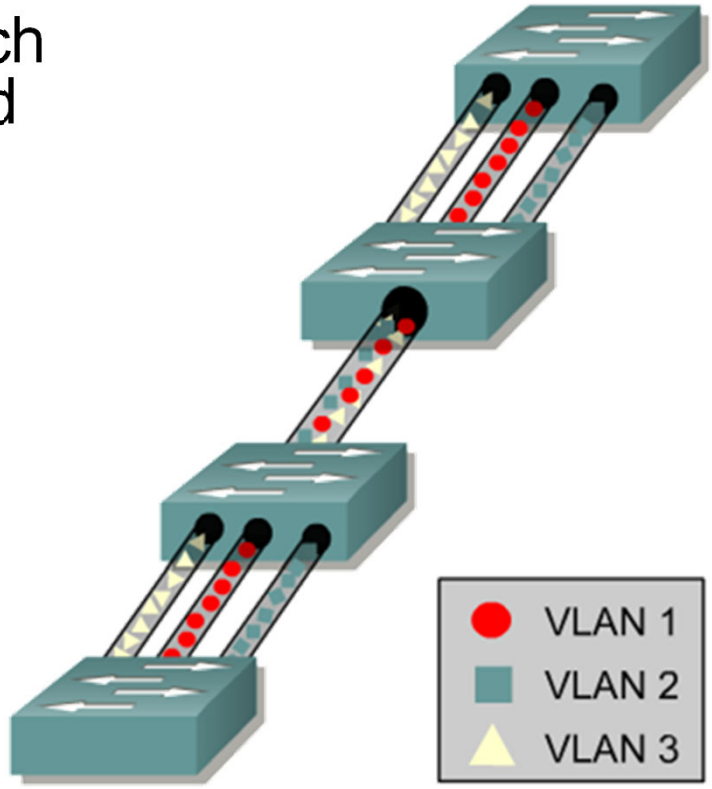
- To configure 802.1q trunking switch/router, first determine which ports on the switches will be used to connect the two switches together
- Then, in the Global configuration mode enter the following commands on both switches:

```
Switch_A(config)#interface fastethernet

                 interface ifnumber


Switch_A(config-if)#switchport trunk

                 encapsulation dot1q
```



Deleting a Port VLAN Membership

```
SydneySwitch#config terminal
SydneySwitch(config)#interface fastethernet 0/9
SydneySwitch(config-if)#switchport access vlan 300
SydneySwitch(config-if)#exit
SydneySwitch(config)#exit
```

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#no switchport access vlan 300
```

```
Switch(config-if)#no switchport access vlan vlan_number
```

Deleting a VLAN

```
Switch #vlan database
Switch(vlan)#no vlan vlan_number
Switch(vlan)#exit
```

Announcement

- Next is Chapter 13 Latest Topics
- 13:30 ~ 15:10 on 21 November (Monday)