Communication Protocols
and Internet Architectures

Harvard University

Lecture #5

Instructor: Len Evenchik
cs40@evenchik.com or evenchik@fas.harvard.edu

ALIGHLSOD1701

Lecture Agenda

- Course Logistics
- Q&A and Topics from Last Week
- IP Routing
- Routing Protocols – RIP and OSPF
- Virtual LANs (VLANs)
- One Minute Wrap-Up

Course Logistics

Course Logistics

- Homework update
- There will be an online midterm exam and an on-campus or proctored final exam. Students in New England must take the final exam on campus while distance students must arrange to have it proctored.
- Please see the syllabus for the dates of the midterm and the final exam.
- **Please submit a one minute wrap-up each week. Thank You!**

© 1998 - 2017 L. Evenchik

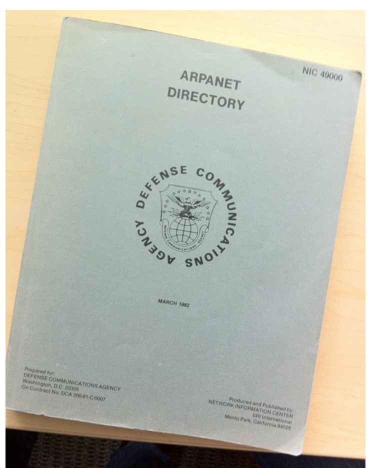
One Minute Wrap-Up

- Please do this Wrap-Up at the end of each lecture.
- Please fill out the form on the website.
- The form is anonymous (but you can include your name if you want.)
- Please answer three questions:
  - What is your grand "Aha" for today's class?
  - What concept did you find most confusing in today's class?
  - What questions should I address next time
- **Thank you!**

Q&A and Some Things from Previous Lectures

© 1998 - 2017 L. Evenchik

Internet History
The Internet Directory: March 1982
(400 pages, 20 names per page)



© 1998 - 2017 L. Evenchik

What is the Internet

- A network of networks with a couple billion users
- With large national and international ISPs (Internet Service Providers) as the core networks
- With regional ISPs connected to national ISPs
- With local ISPs connected to national/regional ISPs
- All ISPs exchanging inbound and outbound traffic with other ISPs across public and/or private peering points.
- With billions of users connected to customer networks at the outer edge, that then connect to one or more of the ISPs.
- *All using the TCP/IP protocol suite*

Changes in Internet Topology

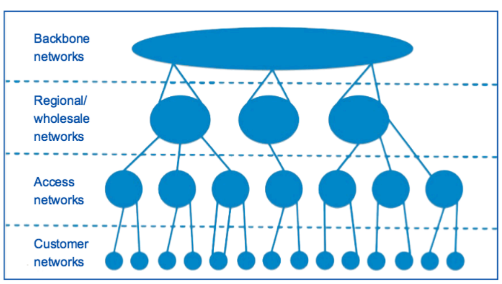


Figure 2 Traditional Internet hierarchical model

Straightforward Hierarchical Topology Early '90s

Mesh or Highly Connected Topology Today, Both ISPs and Others Provide Connectivity as well as Content

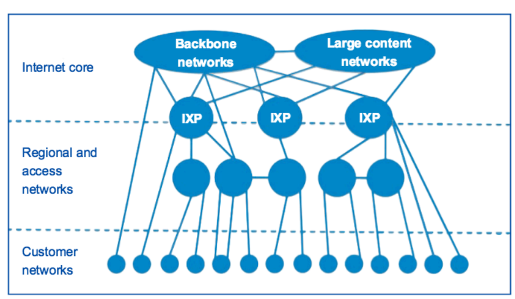
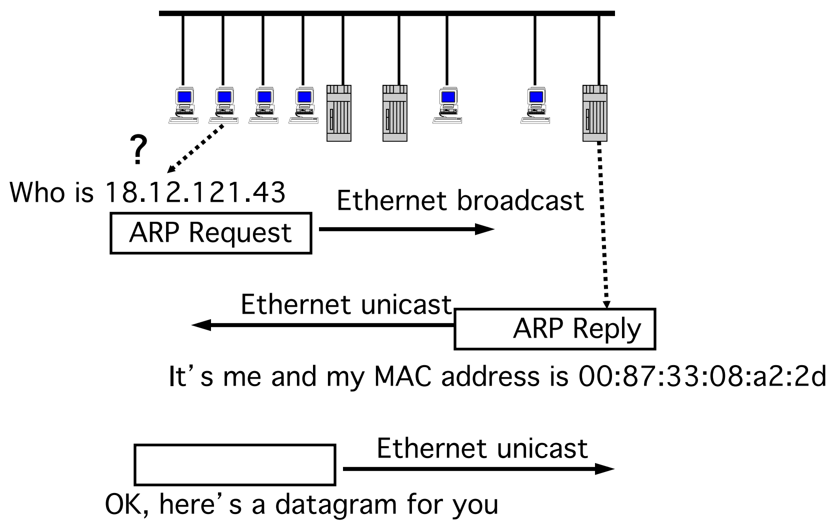


Figure 3 Flatter, more connected model

Source: ISOC Reports

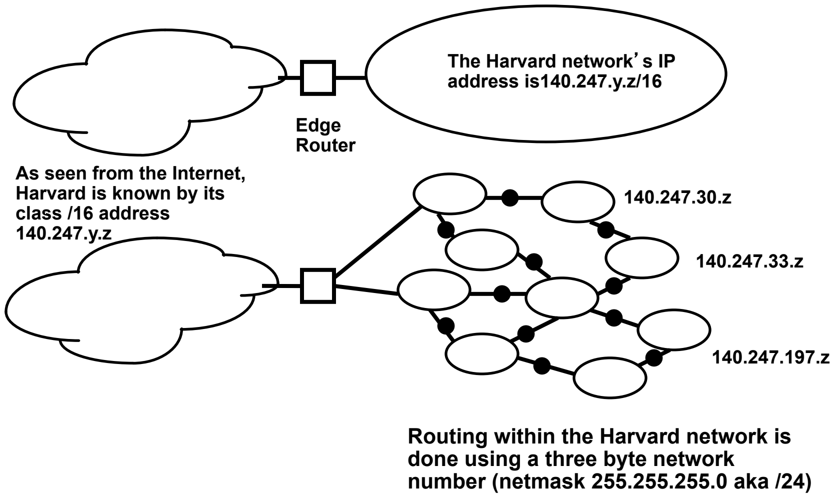
Ethernet ARP Procedure



IPv4 Addressing

CIDR, Network Prefixes, Subnets, etc.

Simplified Subnet Topology
/16 versus /24



Addressing using Network Prefixes

- Address description using the Network Prefix Length format now the norm (but many people still don't know this since they commonly see network masks such as 255.255.255.0 versus /24
- This approach was developed as part of CIDR
- Notation is: address / <prefix length>
  - Class A, networks would be /8 prefix, or 34.2.3.4/8
  - Class B, networks would be /16 prefix, or 140.247.30.33/16
  - Class C, networks would be /24 prefix, or 198.3.4.23/24
- Prefix approach is used for subnetting within an organization.
- Consider 140.247.198/23 as an example

Addressing with Network Prefixes (2)

- Prefix approach is used for subnetting within an organization.
- Consider 140.247.198/23 as an example

Private IPv4 Addresses

Private IP Addresses

(Partial list, more on this in a later lecture)

- Defined in RFC 1918. The title of this RFC is "Address Allocation for Private Internets"
- A better way to think about these addresses is that the are not publicly routable. This means that the public Internet will not route IP packets with these addresses.
- 10/8 10.0.0.0 to 10.255.255.255
- 172.16/12 172.16.0.0 to 172.31.255.255
- 169.254/16 169.254.0.0 to 169.254.255.255
- 192.168/16 192.168.0.0 to 192.168.255.255

ICMP

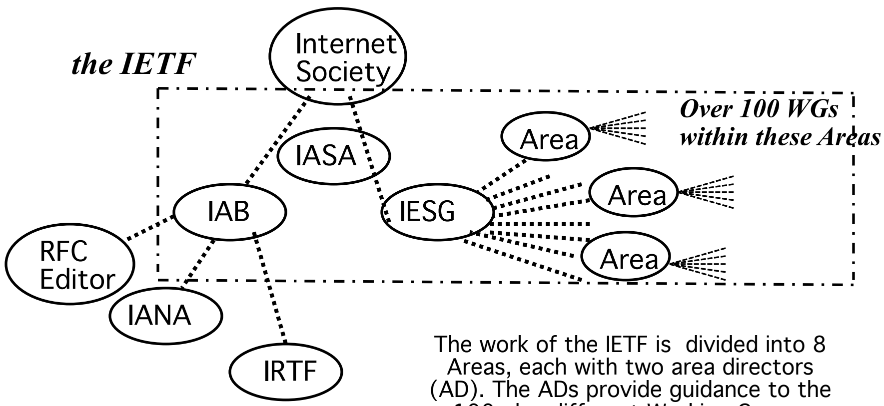
ICMP

- ICMP is an integral part of IP.
- ICMP is used to send debugging information and error reports between hosts, routers and other network devices.
- ICMP messages can be lost or discarded. Errors in ICMP messages should not generate additional ICMP messages. Firewalls today typically block ICMP and this is a big problem.
- ICMP provides very limited functionality. Additional protocols are required for routing, management, and control.
- ICMP includes messages for reporting routing errors, host problems, IP parameter errors, MTU size and fragmentation, and network testing (pinging).
- The software PING and Traceroute use the ICMP protocol.
- **ICMP is important and network devices should support it!**

IETF History, Philosophy, Standards and Procedures

© 1998 - 2017 L. Evenchik

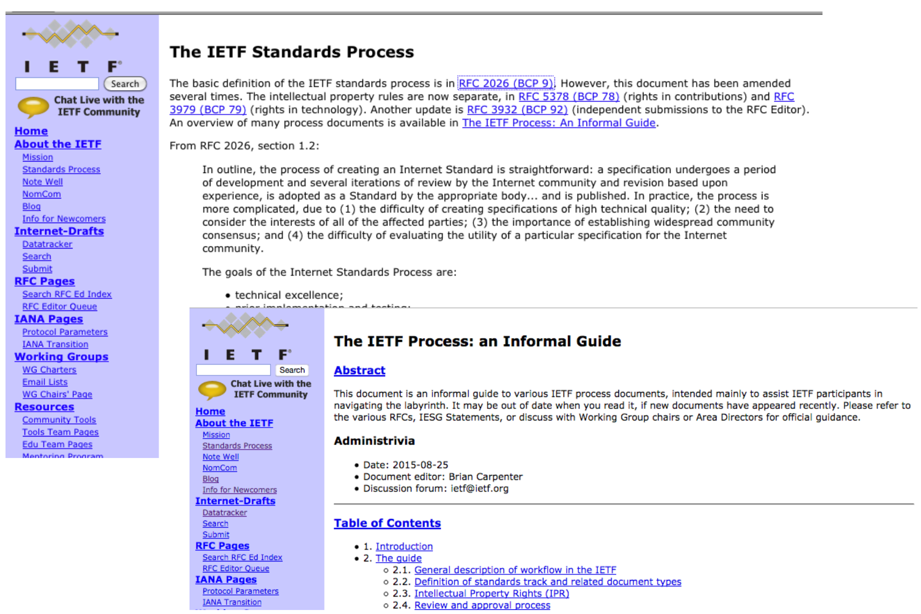
High Level Organizational View



The work of the IETF is divided into 8 Areas, each with two area directors (AD). The ADs provide guidance to the 100 plus different Working Groups.

Source is IETF newcomers presentation.

IETF Standards Process



I E T F

Search

Chat Live with the IETF Community

Home
About the IETF
Mission
Standards Process
Note Well
NomCom
Blog
Info for Newcomers
Internet-Drafts
Datatracker
Search
Submit
RFC Pages
Search RFC Ed Index
RFC Editor Queue
IANA Pages
Protocol Parameters
IANA Transition
Working Groups
WG Charters
Email Lists
WG Chairs' Page
Resources
Community Tools
Tools Team Pages
Edu Team Pages

The IETF Standards Process

The basic definition of the IETF standards process is in RFC 2026 (BCP 9). However, this document has been amended several times. The intellectual property rules are now separate, in RFC 5378 (BCP 78) (rights in contributions) and RFC 3979 (BCP 79) (rights in technology). Another update is RFC 3932 (BCP 92) (independent submissions to the RFC Editor). An overview of many process documents is available in The IETF Process: An Informal Guide.

From RFC 2026, section 1.2:

In outline, the process of creating an Internet Standard is straightforward: a specification undergoes a period of development and several iterations of review by the Internet community and revision based upon experience, is adopted as a Standard by the appropriate body... and is published. In practice, the process is more complicated, due to (1) the difficulty of creating specifications of high technical quality; (2) the need to consider the interests of all of the affected parties; (3) the importance of establishing widespread community consensus; and (4) the difficulty of evaluating the utility of a particular specification for the Internet community.

The goals of the Internet Standards Process are:

- technical excellence;

The IETF Process: an Informal Guide

Abstract

This document is an informal guide to various IETF process documents, intended mainly to assist IETF participants in navigating the labyrinth. It may be out of date when you read it, if new documents have appeared recently. Please refer to the various RFCs, IESG Statements, or discuss with Working Group chairs or Area Directors for official guidance.

Administrivia

- Date: 2015-08-25
- Document editor: Brian Carpenter
- Discussion forum: ietf@ietf.org

Table of Contents

- 1. Introduction
- 2. The guide
  - 2.1. General description of workflow in the IETF
  - 2.2. Definition of standards track and related document types
  - 2.3. Intellectual Property Rights (IPR)
  - 2.4. Review and approval process

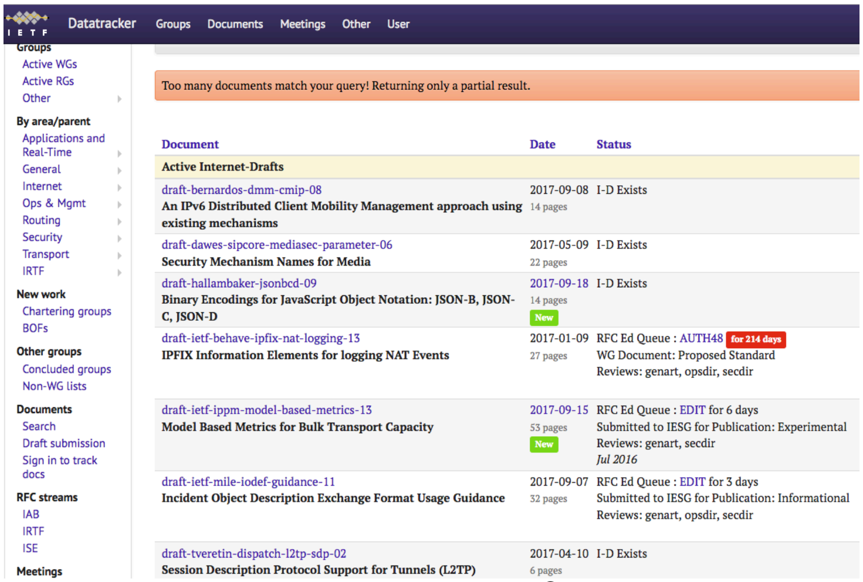
RFCs

- RFC first meant Request for Comments, it is now just a form of publication within the IETF
- The first RFC was in 1969 (RFC#1, Host Software)
- Today, there are many different types of RFCs, many that you would not expect to see
- It is important to understand that not all RFCs are standards
- Now over 5,000 RFCs and counting
- Technical standards track RFCs start out as Internet Drafts (ID.) An ID is not a standard.

Internet-Drafts (IDs)

- IETF working documents are called Internet-Drafts
- There is limited review for documents that are submitted as IDs
- IDs have a stated lifetime of 6 months (but the web means you can always find out-of-date copies.)
- RFCs start out as IDs, but the majority of IDs do not move beyond the ID stage.

There are 1,000s of active Internet-Drafts (IDs)



IETF Standards Process
(Revised by RFC 6410 in 2011)

- Technical documents follow a defined process before they become IETF Standards
- Proposal for a future standard is first published as an ID. It is then refined and updated within a working group.
- Today there is a two step process for an RFC to become an IETF standard. (see RFC 6410)
- First level of the process is called the Proposed Standard
- The second and final level is the Internet Standard
  - As described in RFC 2026: An Internet Standard is characterized by a high degree of technical maturity and by a generally held belief that the specified protocol or service provides significant benefit to the Internet community.

Internet Standards

RFC Editor

Search RFCs

number, title, keyw

Advanced Sea

Official Internet Protocol Standards

This page contains the current lists of

STD 5	RFC 791	ASCII, PDF	**Internet Protocol**	J. Postel	September 1981	Obsoletes RFC 760, Updated by RFC 1349, RFC 2474, RFC 6864, Errata	Internet Standard
STD 5	RFC 792	ASCII, PDF	**Internet Control Message Protocol**	J. Postel	September 1981	Obsoletes RFC 777, Updated by RFC 950, RFC 4884, RFC 6633, RFC 6918, Errata	Internet Standard
STD 5	RFC 950	ASCII, PDF	**Internet Standard Subnetting Procedure**	J.C. Mogul, J. Postel	August 1985	Updates RFC 792, Updated by RFC 6918	Internet Standard
STD 5	RFC 1112	ASCII, PDF	**Host extensions for IP multicasting**	S.E. Deering	August 1989	Obsoletes RFC 988, RFC 1054, Updated by RFC 2236	Internet Standard
STD 5	RFC 919	ASCII, PDF	**Broadcasting Internet Datagrams**	J.C. Mogul	October 1984		Internet Standard
STD 85	RFC 8098	ASCII, PDF	**Message Disposition Notification**	T. Hansen, Ed., A. Melnikov, Ed.	February 2017	Obsoletes RFC 3798, Updates RFC 2046, RFC 3461	Internet Standard
STD 86	RFC 8200	ASCII, PDF	**Internet Protocol, Version 6 (IPv6) Specification**	S. Deering, R. Hinden	July 2017	Obsoletes RFC 2460	Internet Standard
STD 87	RFC 8201	ASCII, PDF	**Path MTU Discovery for IP version 6**	J. McCann, S. Deering, J. Mogul, R. Hinden, Ed.	July 2017	Obsoletes RFC 1981	Internet Standard

© 1998 - 2017 L. Evenchik

Routers and Routing (part 1)

Repeater/Hub versus Bridge/Switch versus Router

- Hub/Repeater (Should not be used to build networks)
  - Improved distance
  - End stations see one physical LAN
  - Single broadcast domain, single collision domain
- Switch/Ethernet Switch/ historical name was bridge
  - End stations see one logical LAN
  - Protocol insensitive
  - Single broadcast domain, multiple collision domains
- Router (sometimes called a L3 Switch)
  - Protocol sensitive (at layer 3)
  - Traffic isolation
  - Multiple broadcast domains, multiple collision domains
  - End stations see multiple networks and of course, multiple LANs

Generic Router Functionality (1)

- Operates at layer 3 and specific layer 3 protocols are supported (or not supported.) This was very important before IP became the dominant layer 3 protocol.
- Router provides multiple collision and broadcast domains
- Router services are requested explicitly by the end stations on the network. End stations send packets to the router only if they need to leave the local network. This is not an easy point to understand.
- Routers support IP fragmentation (IPv4) and other protocol specific network layer functionality

Generic Router Functionality (2)

- Routers are used, of course, for both LANs and WANs
- Routers typically use Access control lists (ACL) for management, router configuration and access control for groups of users.
- As compared to ethernet switches, routers are used in larger, more complex networks. The tradeoff is that routers are more difficult to configure and manage than switches

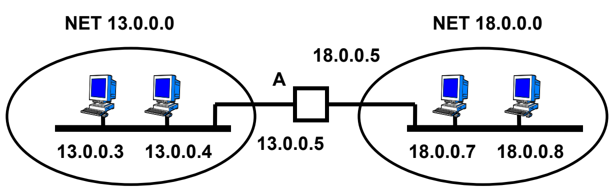
- *…. and of course, routers route packets ….*

© 1998 - 2017 L. Evenchik

What Does a Router Do?

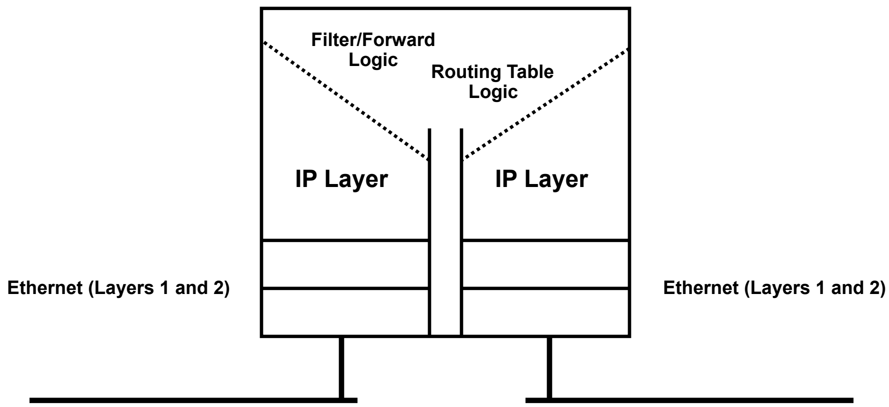
- A router forwards packets based on some understanding of a "next best hop." This information is stored in a forwarding table of some type. (The table is also called a routing table.)
- A router talks to other routers in order to update its table of "next best hop" information. A routing protocol such as RIPv2, OSPF or BGP is used to transfer this information between routers.
- A router implements many different types of management and control functions

Two Network Routing Behavior

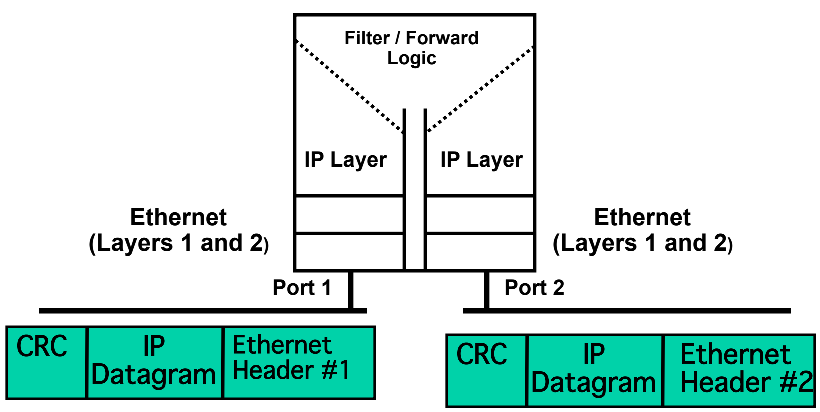


- What is the behavior to reach hosts on the local network?
- What is the behavior to reach hosts on another network?
- How is ARP used in this topology?

Simplified Router Schematic



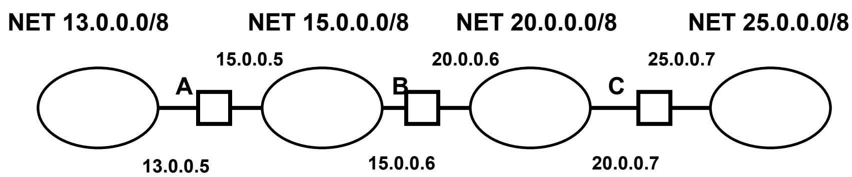
Ethernet Headers are Built Independently on Each Side (Interface) of a Router



Very Simple Router Forwarding Table

Network #	Distance (or cost)	Outgoing Port #	Next Hop IP Address	Etc.,

Multiple Network Simplified Routing Behavior

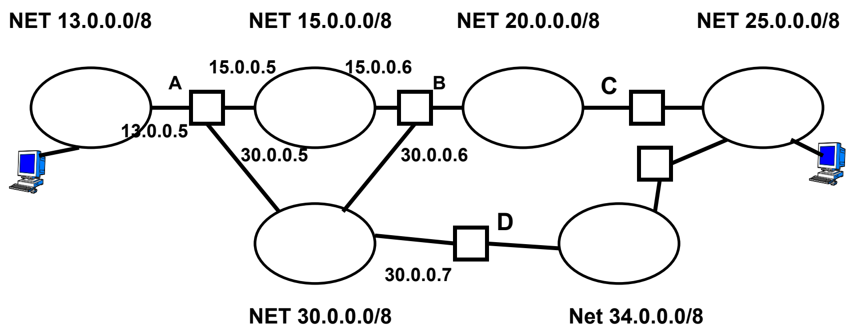


What is in the routing tables of routers A, B and C?

Simplified Router Forwarding Table

Network #	Distance (or cost)	Outgoing Port #	Next Hop IP Address	Etc.,

What Does a Router Do?

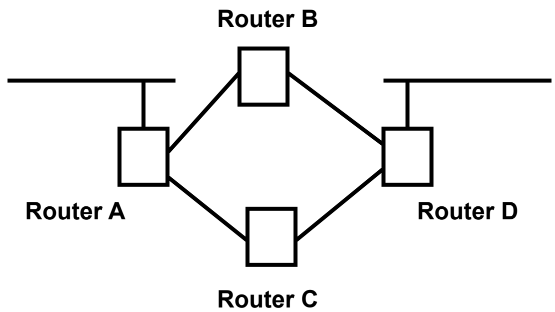


What is in the routing tables of routers A, B, C and D?

Simplified Router Forwarding Table

Network #	Distance (or cost)	Outgoing Port #	Next Hop IP Address	Etc.,

The Basic Routing Decision

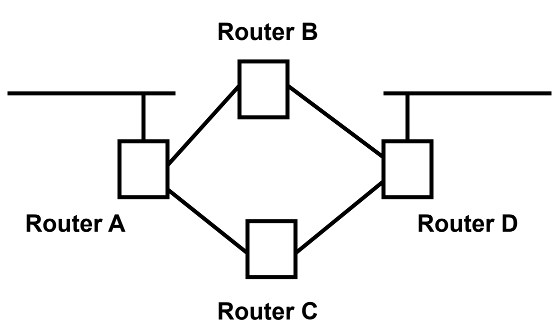


The basic question is where Router A sends the packets destined for stations located off of Router D

© 1998 - 2017 L. Evenchik

Router and Routing Protocols: RIP and OSPF

The Basic Routing Decision



The basic question is where does Router A send the packets destined for stations located off of Router D

Routing Approaches

- Both centralized and distributed approaches are used
- Routing algorithms can be broadly classified as distance-vector or link-state
- Distance vector - good example is RIPv2
  - Cost function is simply based on the number of hops
  - Routers talk to their neighbors only
  - Historical note: No subnet masks in the original RIPv1
- Link state - good example is OSPF
  - "Complex" cost function for links
  - Routers flood their link state to all routers within AS
  - Packets include IP address prefix information

Routing Information Protocol (RIPv1) Some Historical Information

- RIP was an IGP based on work originally done at Xerox PARC for XNS about 40 years ago. Berkeley UNIX version was known as "routed" and it was distributed as part of UNIX. This is the reason it became so popular.
- RIP (v1 and v2) implement distance vector routing.
- The complete routing database is broadcast from each router every 30 seconds.
- Network ID and hop-count sent for each entry in the database
- RIP (v1 and v2) are not good at detecting loops
- Hop count does not define delay
- RIPv2 is the current version for IPv4. RIPng is for IPv6.

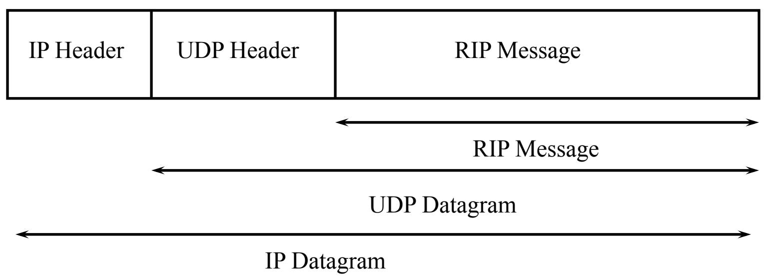
RIPv2 Features (1)

- RIPv2 is documented in RFC 2453, November 1998
- RIPv2 is still a basic distance vector routing protocol, uses UDP, max hop count is 15 and 16 is infinity. Hop count is different than the number of routers in the network.
- Very simple unencrypted authentication feature is available
- Each router sends out an update every 30 seconds, or when triggered by a topology change
- Address prefixes and subnet support are handled by including subnet mask
- Each router builds its own table of what the network looks like, and how best to route packets.

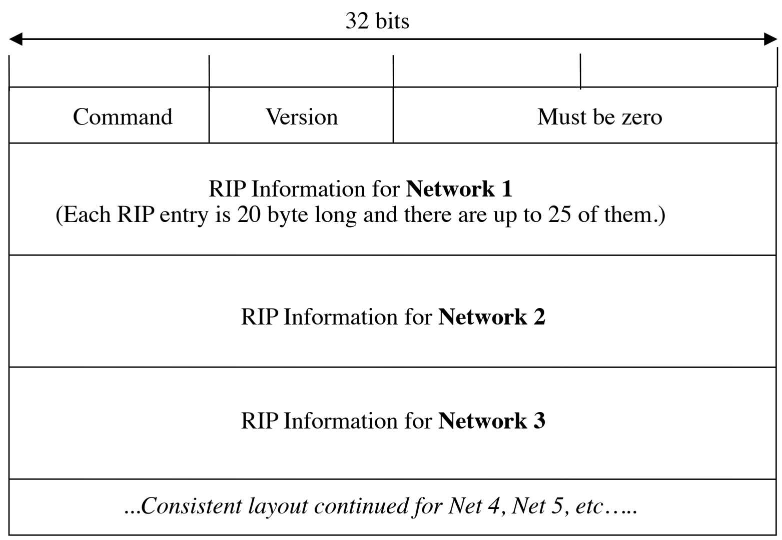
RIPv2 Features (2)

- Each router builds its own table of what the network looks like and how best to route packets. This means that the routing table in each router is different.
- The RIPv2 messages that are sent every 30 seconds are a complete snapshot of the routing table
- Network address and hop-count are sent for each entry in the database (as they were in RIPv1)
- Next Hop field is added to each Route Table Entry (RTE)
- Route Tag is added to each Route Table Entry
- RIP uses UDP and is assigned UDP port 520

RIP Encapsulation



RIP Packet: Details Included on Multiple Nets



RIPv2 Packet Format

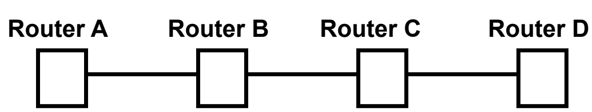
32 bits

Command	Version	Must be zero	
Address Family of Net 1 (IP=2)		Route Tag	
IP Address of Net 1			
Subnet Mask			
Next Hop			
Metric, Distance to Net 1			
Address Family of Net 2		Must be zero	
IP Address of Net 2			

...Consistent layout continued for Net 2, Net 3, etc…..

RIP and “Bad News”

Review the Literation for the Count to Infinity Problem in RIP



Time	A	B	C	D
0				
1				
2				
3				

OSPF - Open Shortest Path First (1)

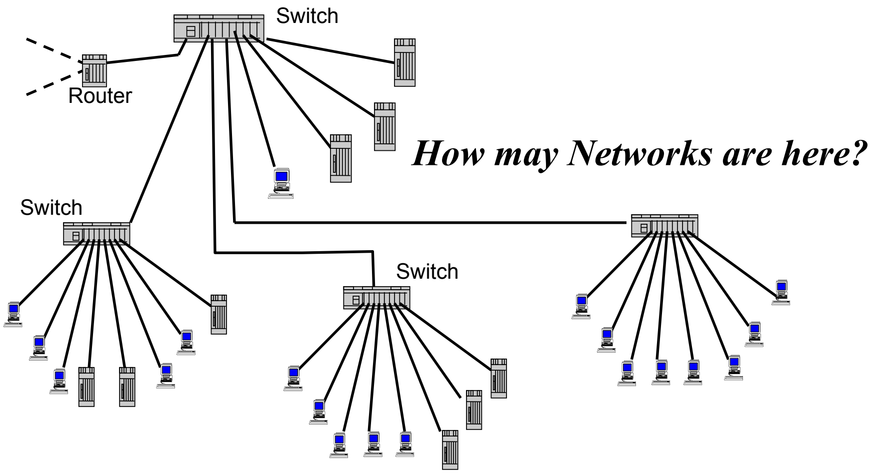
- OSPF uses "complex" cost functions for link state rather than hop count, but the simpler the cost function the better
- Encapsulated within IP directly (does not use UDP or TCP)
- OSPF supports multiple types of routes
- Updates are authenticated
- Networks may be partitioned into multiple areas for easier management, and OSPF runs "independently" within each area

OSPF - Open Shortest Path First (2)

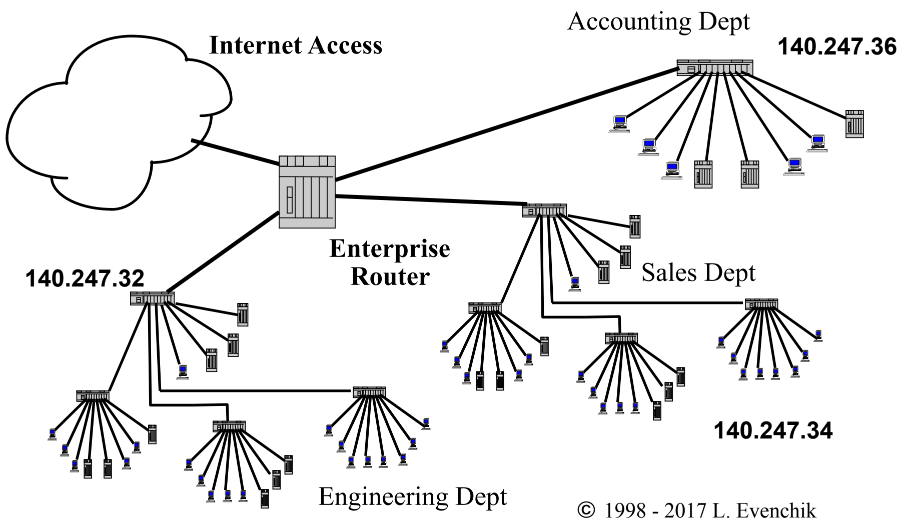
- Link state updates are sent whenever the router's link information changes
- The updates only include information on the links that the router knows about explicitly. (The links that it is directly connected to.)
- Subnet masks are associated with each advertised route
- Link updates are flooded so that all the routers learn the link information for each router in the network
- All the routers in the network aggregate the information and build a (hopefully) consistent view of the network

Virtual LANs (VLANs) 802.1P & 802.1Q

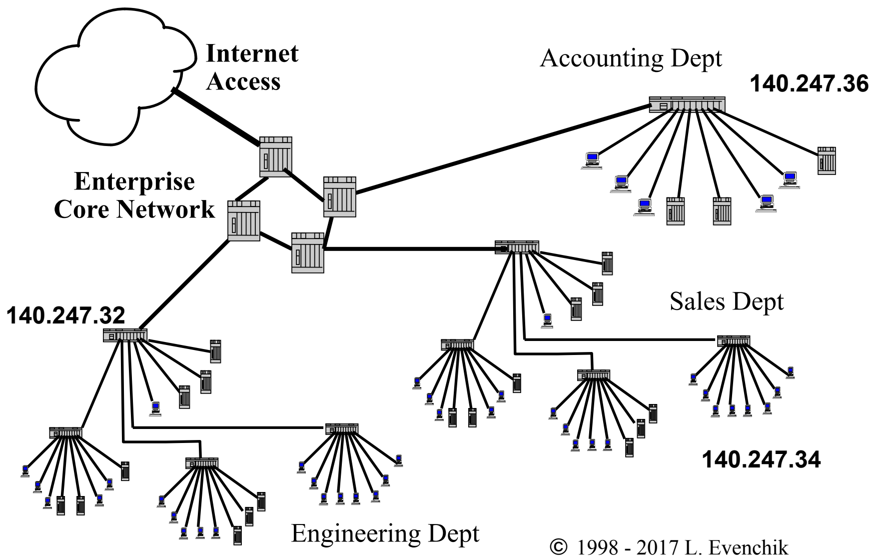
Generic LAN Topology



Common LAN Architecture with a Number of Subnets



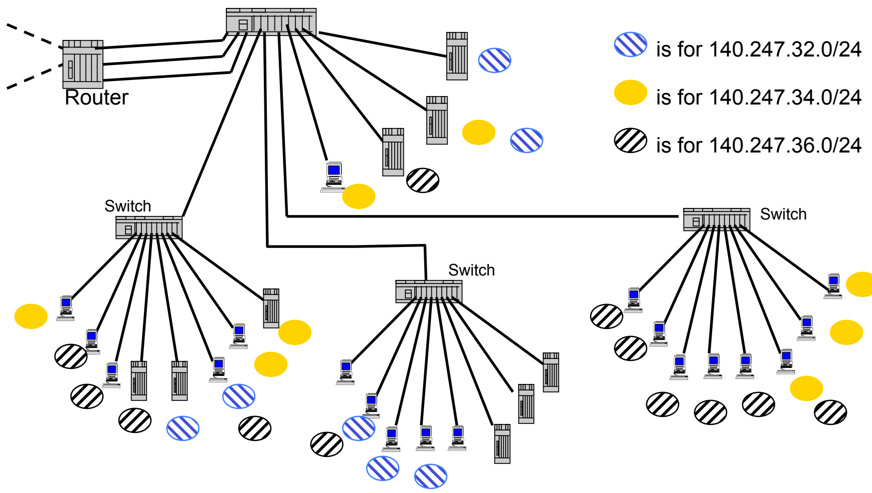
Common LAN Architecture (2)



Rational for Virtual LANs

- Groups of users within an organization are typically separated into their own IP networks for network management, performance, security and other policy reasons.
- From a business perspective, this means that users on LANs should be grouped into separate networks by their community of interest (sales dept., engineering, accounting), not by their office location within the building.
- However, it is rare that all the users within a single community of interest are located in the same part of a building.
- From a technical perspective, "Ethernet switches are easy, routers are hard."
- Given all the above, how can we separate users via ethernet switches versus routers? This was the question about 20 years ago, which is when VLANs were developed.

Ethernet Switch and VLAN Topology



Note that it is common to talk about colors when talking about VLANS, but networks do not have colors, they have network numbers.

Virtual LANs (1)

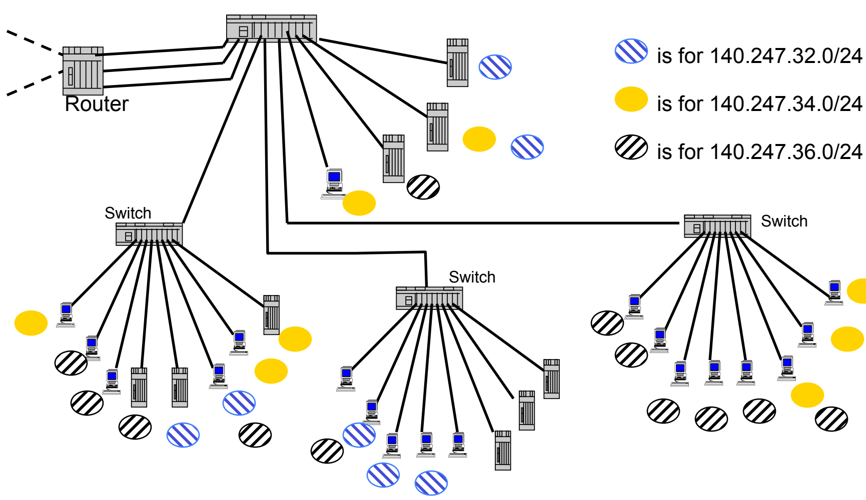
"Switches are easy, routers are hard." Given this, how can we separate users via switches? What are the benefits?

- Virtual LANs assign users to a specific IP network regardless of the ethernet switch, or the port on a particular switch, that the user is physically connected to.
- This means that different users on the same ethernet switch can be members of different networks. In other words, one switch can support multiple IP networks.
- Each network (or subnet) has a different IP network number and therefore provides a separate broadcast domain.
- The switches maintain VLAN configuration information which identifies which switch ports, and/or which users, are members of each VLAN, i.e., individual IP network.

Virtual LANs (2)

- The switches maintain VLAN configuration information which identifies which switch ports, and/or which users, are members of each VLAN, i.e., individual IP network.
- By using VLANs, one IP network can span multiple switches and multiple locations.
- Users are assigned to a VLAN by a network administrator, or automatically via a management system. Auto-configuration requires a policy such as, "all users on switch ports 1 to 5 are on the accounting network"
- The term VLAN can be confusing since it mixes together two different things: LAN topology, and assigning users to a particular IP network.
- Given that users on different VLANs are on different IP networks, how do they talk to each other?

Ethernet Switch and VLAN Topology

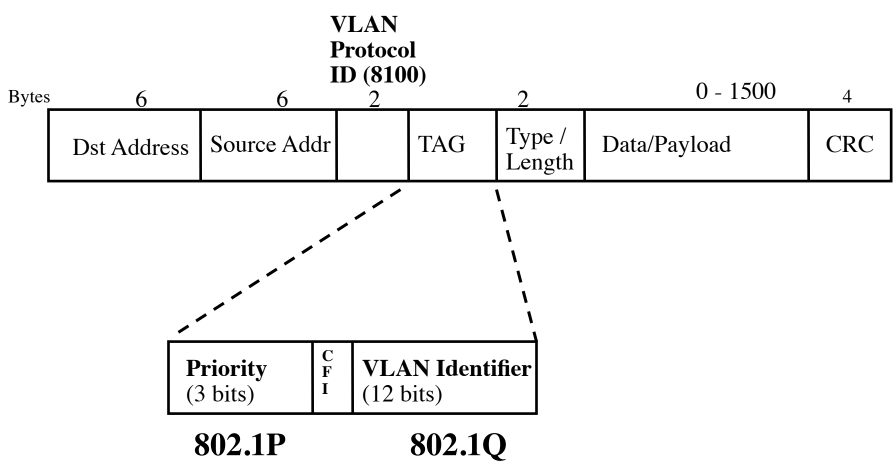


Note that it is common to talk about colors when talking about VLANS, but networks do not have colors, they have network numbers.

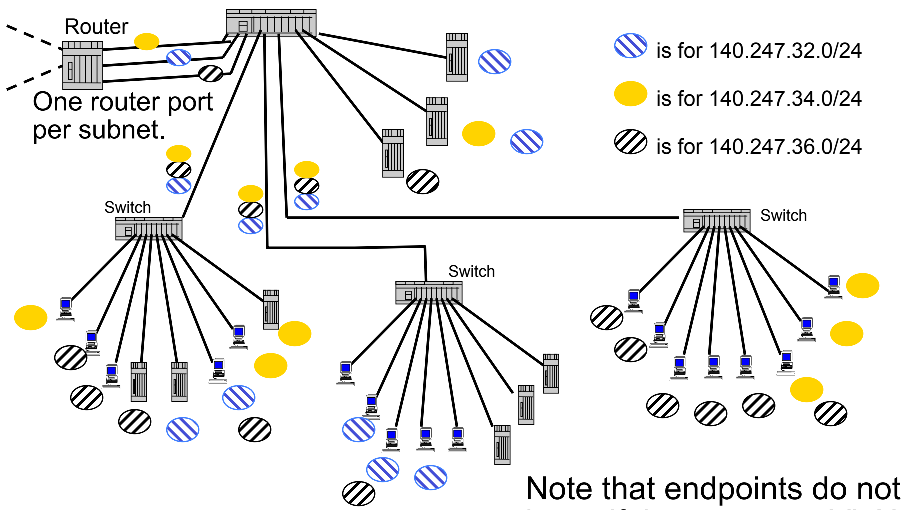
Virtual LANs – 802.1q

- VLANs are identified by a 12 bit VLAN Identifier. It is common to talk about VLAN colors, but there are no colors. A VLAN tag is a number.
- Devices connected to a switch are assigned, or put into a specific VLAN, based on one or more of the following:
  - Switch Port – all devices on this port are on a specific VLAN
  - MAC address of the sending station
  - IP address of the device
  - Type of traffic on that port – specific VLAN for wireless traffic
  - Specific user that is currently logged into a device
  - Other IP and/or TCP information
  - Combination of the above
- Ethernet priority and VLANs are distinct concepts, but they are intertwined by the technology.

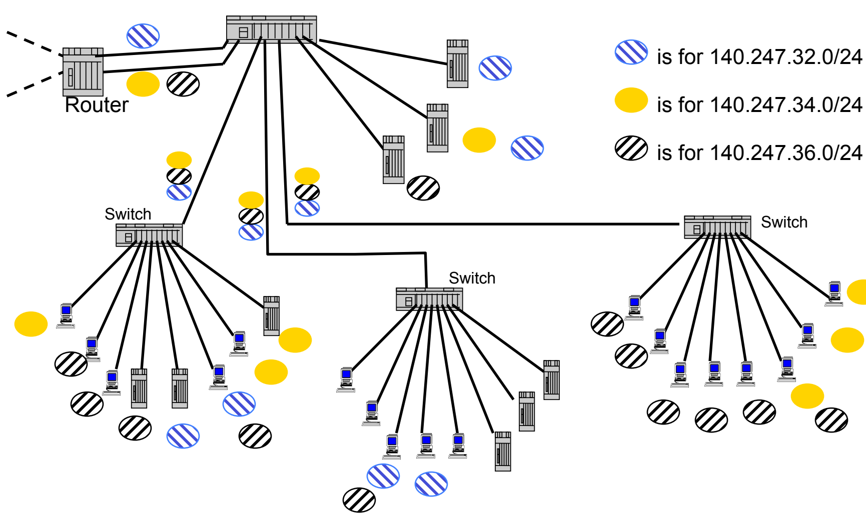
IEEE 802.1 P / Q Frame Format



Simplistic Router and VLAN Topology



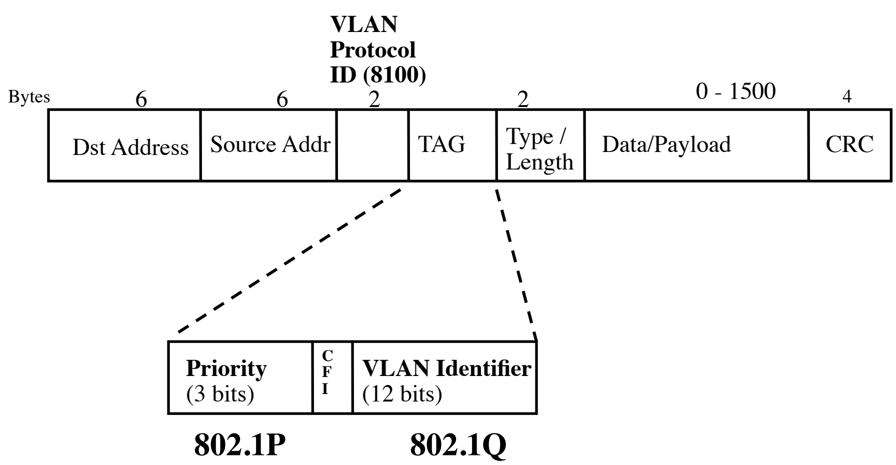
Typical Router Support for VLAN Tags



802.1p and Virtual LANs

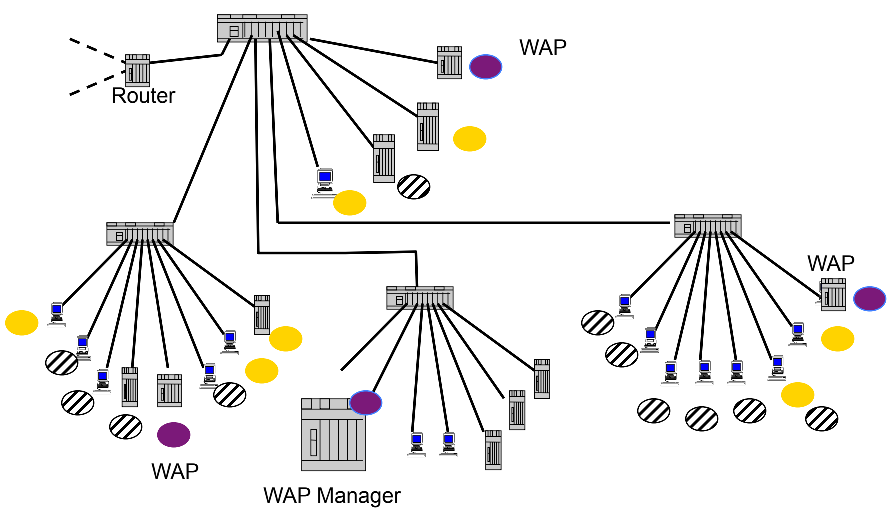
- Ethernet priority and VLANs are distinct concepts, but they are intertwined by the technology.
- Frame priority is marked by a 3 bit field, 0 to 7. This is known as Class of Service.
- Switches can and do, write or re-write, the priority field based on:
  - Port on which the frame was received
  - MAC address of the sending station
  - Protocol or traffic type – web, streaming media, real time video
  - IP Precedence field or DSCP
  - Other IP and/or TCP information
  - Combination of the above

IEEE 802.1P Format Specifies a Priority



Wireless LANs and VLANs

Wireless Networks and VLAN Topology



Advantages of VLANs

- Separates physical location from a user's network identity
- Better isolation between groups of users: however it is incorrect to think that VLANs significantly improve network security.
- Improved performance: the specific LAN performance requirements of each group can be met more easily.
- Improved performance: VLANs provide multiple broadcast domains
- VLANs allows for sophisticated network administration, without the complexity of routers

Virtual LANs
Some Quick Questions

- Can VLANs span multiple sites, such as different buildings on a campus?
- What is the best way to assign users to VLANs?
- Does a client machine know if it is on a VLAN?
- How do users on different VLANs talk to each other?

Thank You!

ALIGHLSOD1701

One Minute Wrap-Up

- Please do this Wrap-Up at the end of each lecture.
- Please fill out the form on the website.
- The form is anonymous (but you can include your name if you want.)
- Please answer three questions:
  - What is your grand "Aha" for today's class?
  - What concept did you find most confusing in today's class?
  - What questions should I address next time
- **Thank you!**