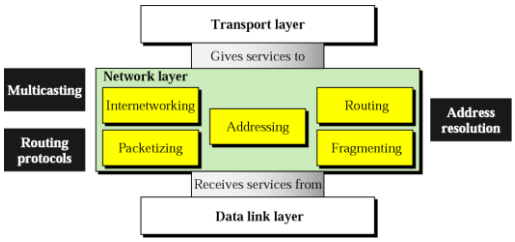
Chapter 4: Network Layer

Introduction to Network Layer

- Layer 3 or Network Layer is backbone of the OSI model
- It finds the best path for data transfer between nodes
- It manages device addressing

Position and Function of Network Layer



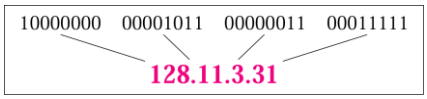
Design Issues at the Network Layer

- Switching Technique:
  - Datagram
  - Virtual circuits
- Routing:
  - How to forward packets
  - How to calculate a path from source to destination?
- Traffic Control:
  - Congestion control
  - Rate control

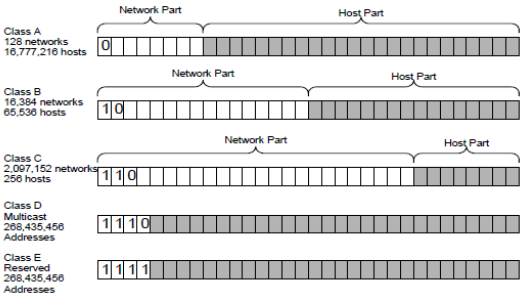
- Naming and Addressing:
  - How to find the name of a network node?
- Internetworking:
  - How to interconnect heterogeneous networks?

IPV4 Address

- 32 bit address
- Total unique address equals to 2^32
  - Around 4.2 billion address
- Represented in dotted Decimal Format
- IANA has authority for IP address management

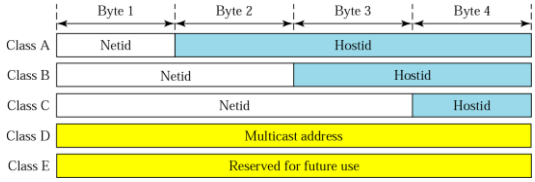


Classful Addressing



7

Network Id and Host Id in Classful addressing



8

Default subnet mask for Classful address

Class	*In Binary*	*In Dotted-Decimal*	*Using Slash*
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

9

- Logical Address:
  - IP address at the Network Layer
  - Used to Communicate with the different subnets
- Netid: Identify network
- Hostid: Identify End devices
- Mask: Used to find netid and hostid
- CIDR: Classless interdomain routing
  - Used in classless addressing
  - Defined by slash notation /n
  - Example: /8, /16, /24

10

Subnetting and Supernetting

- Subnetting:
  - Method used to divide the addresses into several contiguous groups (network)
- Supernetting:
  - Several Network are combined to create a SuperNetwork
  - Mainly used to combine several class C blocks to create a large range of address
  - Supernetting decrease the number of 1s in the mask

11

Classless Addressing

- To overcome address depletion, classless concept is used
- For classless addressing
  - The address in a block must be contiguous
  - The number of address in a block must be power of 2

12

Private IP Address

- Range of IP address, which are not routable to internet commonly used for home, office, and enterprise local area networks (LANs)
- If such a private network needs to connect to the Internet, it must use either a network address translator (NAT) gateway, or a proxy server.

	Range
Class A	10.0.0.0 - 10.255.255.255
Class B	172.16.0.0 - 172.31.255.255
Class C	192.168.0.0 - 192.168.255.255

13

Introduction to IPV6

- Major points that played a key role in the birth of IPv6 (drawback of IPV4):
  - Internet has grown exponentially
    - ➢address space allowed by IPv4 is saturating.
  - There is a requirement to have a protocol that can satisfy the needs of future Internet addresses
  - IPv4 on its own does not provide any security features.
    - ➢Data has to be encrypted with some other security application before being sent on the Internet.

14

- IPv4 enabled clients can be configured manually or they need some address configuration mechanism.
  - ➢It does not have a mechanism to configure a device to have globally unique IP address.

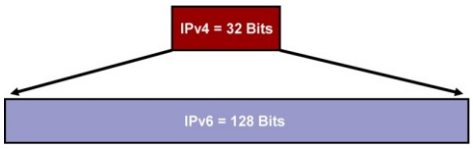
15

Why IPv6?/Advantages of IPV6

- Because of IP shortage in IPV4, IPV6 was introduced with following benefits:
  - Expanded addressing capabilities
  - Structured hierarchy to manage routing table growth
  - Serverless auto configuration and reconfiguration
  - Streamlined header format and flow identification
  - Improved support for options / extensions
  - Security (IPsec mandatory)

16

IPv6 Address



- IPv4: 32 bits or 4 bytes long
  - 4,200,000,000 possible addressable nodes
- IPv6: 128 bits or 16 bytes
  - 3.4 * 10^{38} possible addressable nodes
  - 340,282,366,920,938,463,374,607,432,768,211,456
  - 5 * 10^{28} addresses per person

17

128-bit IPv6 Address

3FFE:085B:1F1F:0000:0000:0000:00A9:1234

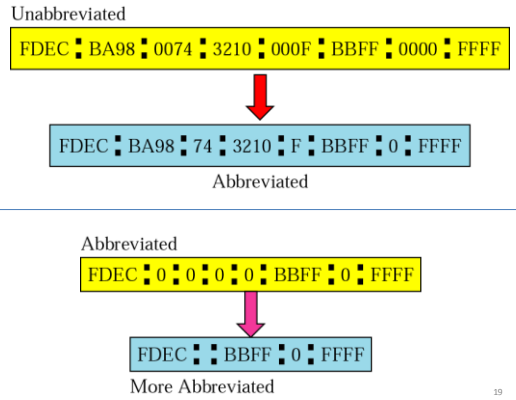
8 groups of 16-bit hexadecimal numbers separated by ":"

Leading zeros can be removed

3FFE:85B:1F1F::A9:1234

:: = all zeros in one or more group of 16-bit hexadecimal numbers

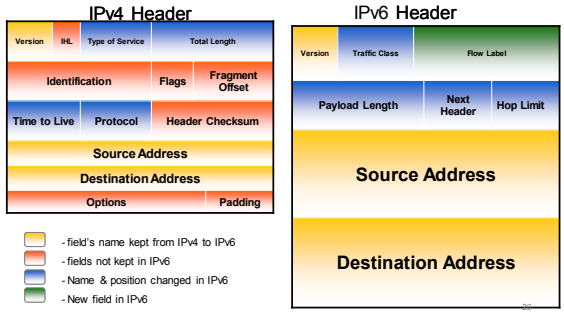
18



19

IPv4 & IPv6 Header Comparison

IPv4: 20 Bytes + Options IPv6: 40 Bytes + Extension Header



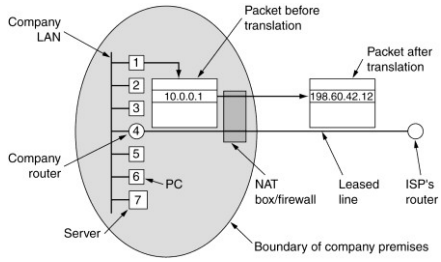
20

Comparison of IPV4 and IPV6 Addressing

IPV4	IPV6
IPV4 addresses are 32 bit	IPV6 addresses are 128 bit
IPV4 are represented in dotted decimal format	IPV6 addresses are represented in hexadecimal format separated by colon(:)
IPSec support is only optional	Inbuilt IPSec support
Fragmentation is done by senders and forwarding routers	Fragmentation is done by sender
No packet flow identification	Packet Flow identification is available using Flow Label field
Checksum field is available in IPV4 header	No checksum field in IPV6 header
IPV4 configuration is done manually or using DHCP	Auto-configuration addresses is available
Options field is available	No options field but IPV6 extension header are available
Limited address space	Large addressing space
Broadcast address are available	No broadcast, its function is superseded by multicast address

21

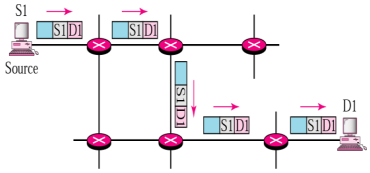
NAT – Network Address Translation



22

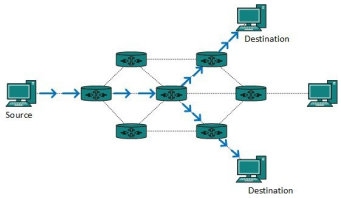
Example Addresses: Unicast, Multicast and Broadcast

- Unicast
  - Useful when there is a participation of single sender and single receiver



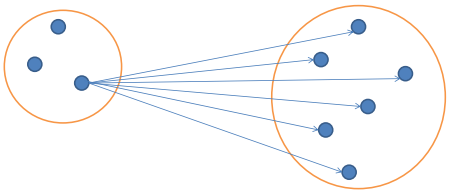
23

- Multicast
  - In multicasting there is at least one sender and several receivers (group of receivers called multicast group)
  - M-cast group address "delivered" to all receivers in the group
  - Internet uses Class D for m-cast
  - M-cast address distribution, etc. managed by IGMP Protocol



24

- Broadcast
  - It sends packet to all the connected devices over the network
  - Useful in television and radio broadcasting



25

Routing

- The process of moving a packet of data from source to destination is called routing.
- It is performed by a dedicated device called router

Criteria for good routing

- Correctness, Complexity (few time, storage, messages to compute tables), Efficiency, Robustness, adaptive, fairness in delivery of packets

26

Static routing

- Static routes are manually entered into a router or host.
- An administrator must know the internetwork layout and the paths that exist between networks.
- Then the administrator must program each router in the internetwork with the proper routes to get from any given network to any other network.
- The hosts obtain their routes manually or via DHCP.

27

Dynamic routing

- Dynamic routes are routes learned via one or more routing protocols.
- Routing protocols are used by routers to inform one another of the IP networks accessible to them.
- There are classful routing protocols, such as RIPv1, that do not transmit masks in their routing updates - the classful network mask is implied.
- There are also classless routing protocols, such as OSPF, that do transmit masks in their routing updates.
- Routing protocols typically do not apply to hosts.
  - Hosts obtain their routes by manual configuration or by DHCP.

28

Static vs dynamic routing

- static routes are entered manually and the dynamic routes are learned and/or calculated dynamically.
- A statically routed network has almost no way of adapting to temporary topology changes. But dynamic routing protocols are designed for this purpose.
- Advantages of Static Routing
  - Minimal CPU/Memory overhead
  - No bandwidth overhead (updates are not shared between routers)
  - Granular control on how traffic is routed

29

- Disadvantages of Static Routing
  - Infrastructure changes must be manually adjusted
  - No “dynamic” fault tolerance if a link goes down
  - Impractical on large network
- Advantages of Dynamic Routing
  - Simpler to configure on larger networks
  - Will dynamically choose a different (or better) route if a link goes down
  - Ability to load balance between multiple links

30

- Disadvantages of Dynamic Routing
  - Updates are shared between routers, thus consuming bandwidth
  - Routing protocols put additional load on router CPU/RAM
  - The choice of the "best route" is in the hands of the routing protocol, and not the network administrator

31

Interior Routing Protocols

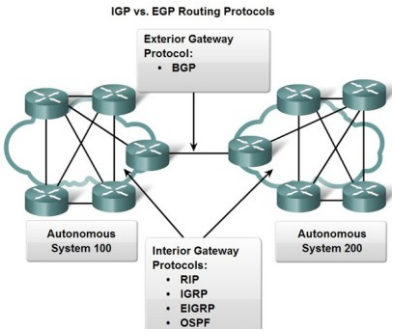
- Used for Routing Inside an Autonomous System (AS).
- Used within the Organization
- AS => Network under Common Administration.
- Router having Same AS, share their routing tables
- Examples => RIP, EIGRP and OSPF, IGRP

Exterior Routing Protocols

- Used for Routing between Autonomous System (AS)
- Border Gateway Routing Protocols (BGP)
- Used between the organization (ISPs to ISPs)

32

Example



33

Distance Vector Routing vs Link state Routing

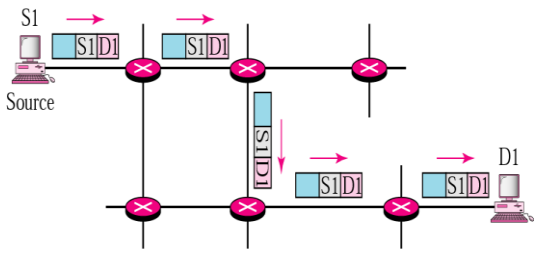
Distance Vector Routing	Link State Routing
Uses Bellman Ford Algorithm	Uses Dijkstra's Algorithm
Practical implementation is RIP and IGRP	Practical implementation is OSPF
Configurations is easy	Configurations is difficult
Bandwidth required is less due to local sharing, small packets and no sharing	Bandwidth required is more due to flooding and large link state packets
Based on local knowledge since its update is based on information from neighbors	Based on global knowledge i.e., it has knowledge of entire network
Less CPU and memory utilization	More CPU and memory utilization
Traffic is less	Traffic is more

34

Unicast Routing

- In unicasting there is a single sender (source) and a single receiver (destination)
- In unicast routing, the router forwards the received packet through only one of its interfaces
- Examples of Unicast Routing are
  - ➢OSPF
  - ➢RIP
  - ➢BGP

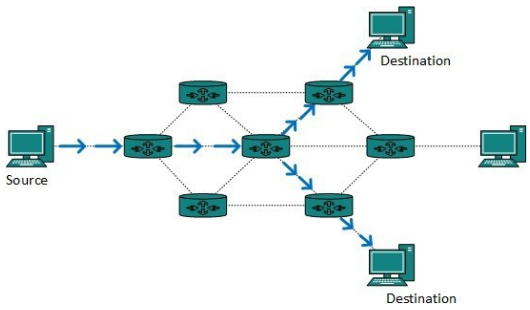
35



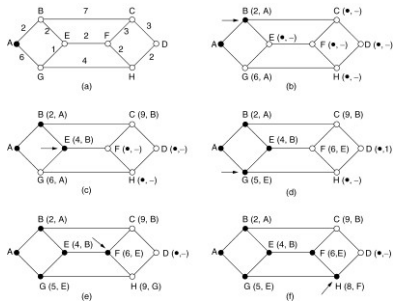
36

MultiCast Routing

- In multicasting there is at least one sender and several receivers (group of receivers called multicast group)
- In multicast routing, the router may forward the received packet through several of its interfaces.
- M-cast group address "delivered" to all receivers in the group
- Internet uses Class D for m-cast
- M-cast address distribution, etc. managed by IGMP Protocol



Dijkstra's Shortest Path Routing



The first 5 steps used in computing the shortest path from A to D.
The arrows indicate the working node.

- To send a packet from one node to another find the shortest path between the pair of nodes
- This is possible due to Dijkstra
  - Initially, no paths are known, so all nodes are labeled with infinity.
  - As the algorithm proceeds and paths are found
    - ➢the labels may change, reflecting better paths.
    - ➢A label may be either tentative or permanent.
    - ➢Initially, all labels are tentative.
    - ➢When it is discovered that a label represents the shortest possible path from the source to that node, it is made permanent and never changed thereafter.

Bellman Ford Routing

- Refer to class notes

Routing Protocols

RIP

- Routing Information Protocol
- RIP is a routing protocol for exchanging routing table information between routers.
- Routing updates must be passed between routers so that they can make the proper choice on how to route a packet
- Oldest Distance Vector Routing Protocol
- Update routing table every 30 sec

- Use Hop count as Metric to find best path to the destination
  - RIP has a maximum hop count of 15
  - A route with a hop count greater than 15 is considered unreachable
- It has two version
  - RIP Version 1
  - RIP Version 2
- RIP version 1 is the classful routing protocol
- RIP Version 2 is classless routing protocol
- In fact, most DSL/cable modem routers such as the ones from Linksys come bundled with RIP.

43

General Operation :RIP

- General packet handling
  - if any of the must-be-zero fields have nonzero values anywhere or if the version field is zero, the packet is discarded.
- Initialization
  - when a router is activated and it determines that all the interfaces are alive, and it broadcasts a request message that goes to all interfaces in the "request-full" mode.
  - Once the responses are received, the routing table is updated with new routes the router has learned about.
- Normal routing updates
  - In the default case, this is done approximately every 30 sec (*"Autoupdate timer")*

44

- Normal response received
  - the routing table is updated by doing the distributed Bellman– Ford step
  - only a single best route is stored for each destination
- Triggered updates
  - if the metric for an addressable network changes, an update message is generated containing only the affected networks
- Route expiration
  - if an addressable network has not been updated for 3 min (*"expiration timer") in the default case, its metric is set to infinity and it is a candidate for deletion.*

45

OSPF

- Open shortest path first protocol
- Classless routing protocol
- routing protocol for Internet Protocol (IP) networks
- uses a link state routing algorithm and falls into the group of interior routing protocols
- OSPF was developed as a replacement for the distance vector routing protocol RIP
- Use cost to find the best route to find the destination

46

- Every intra-domain must have a core area
  - It is referred to as a *backbone area*
  - This is identified with Area ID 0
  - Areas are identified through a 32-bit area field
  - Thus Area ID 0 is the same as 0.0.0.0
- Areas (other than the backbone) are sequentially numbered as Area 1 (i.e., 0.0.0.1), Area 2, and so on

47

OSPF Hello Packets

- The OSPF Hello packet is used to establish neighbor adjacencies. By default, OSPF Hello packets are sent
  - Every 10 seconds on multi-access and point-to-point segments
  - Every 30 seconds on non-broadcast multi-access (NBMA) segments (Frame Relay, X.25, ATM).

OSPF Dead Intervals

- OSPF dead interval is measured as the period of time an OSPF router will wait before terminating adjacency with a neighbor.
- The Dead interval is four times the Hello interval, by default.

48

BGP

- Border Gateway Routing Protocols
- Designed to exchange routing and reachability information between autonomous systems (AS) on the Internet
- Two types
  - Internal BGP
  - External BGP
- Internal BGP has the Administrative Distance of 200
- External BGP has the Administrative Distance of 20

49

- The protocol is often classified as a path vector protocol, but is sometimes also classed as a distance-vector routing protocol.

PATH VECTOR PROTOCOL

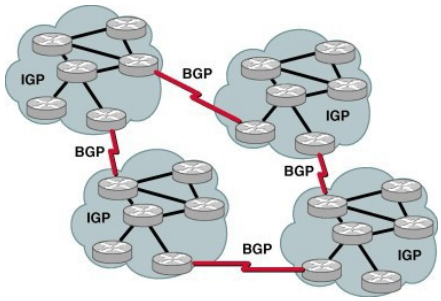
- routing protocol which maintains the path information that gets updated dynamically.
- Updates which have looped through the network and returned to the same node are easily detected and discarded.

50

BGP contd..

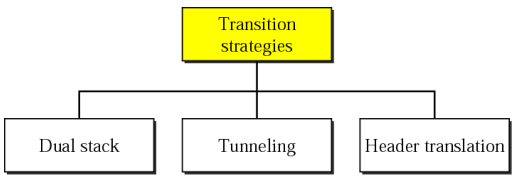
- Peers exchange BGP messages using TCP
- BGP defines 4 types of messages:
  - OPEN: opens a TCP connection to peer and authenticates sender
  - UPDATE: advertises new path (or withdraws old)
  - KEEPALIVE: keeps connection alive in absence of UPDATES; also serves as ACK to an OPEN request
  - NOTIFICATION: reports errors in previous message; also used to close a connection

51



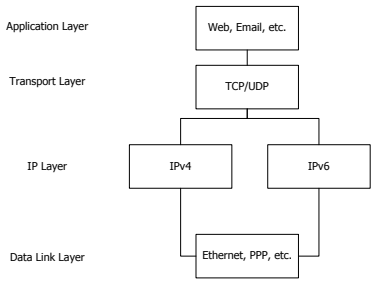
52

Transition from IPv4 to IPv6



53

Dual Stack



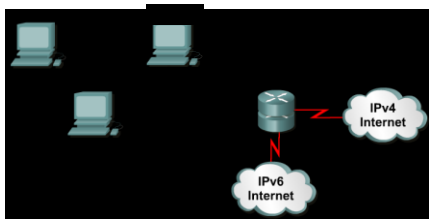
54

Dual Stack contd..

- This allows all the end hosts and intermediate network devices (like routers, switches, modems etc.) to have both IPv4 and IPv6 addresses and protocol stack.
- If both the end stations support IPv6, they can communicate using IPv6
  - otherwise they will communicate using IPv4.
- This will allow both IPv4 and IPv6 to coexist and slow transition from IPv4 to IPv6 can happen.
- Equipment will prefer IPv6 from IPv4 if both are possible.
- When adding IPv6 to a system, do not delete IPv4
  - This multi-protocol approach is familiar and well-understood
  - In most cases, IPv6 will be bundled with new OS releases

55

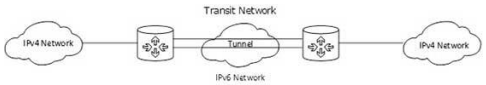
Dual Stack Hosts and Network



56

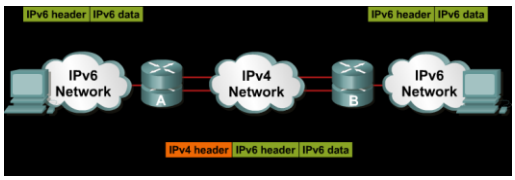
Tunneling

- when different IP versions exist on intermediate path or transit networks
  - tunneling provides a better solution where user's data can pass through a non-supported IP version.
- The diagram depicts how two remote IPv4 networks can communicate via a Tunnel, where the transit network was on IPv6.



57

Tunneling IP6 via IP4



58

Tunnelling Mechanisms

- How they work:
  - Encapsulation of IPv6 packets within IPv4 packets and vice versa
    - ➢Which means it can also be used for IPv4 connections over IPv6 native networks
- Many methods exist for establishing tunnels:
  - manual configuration (manual configurations in both sides)
  - tunnel brokers (using web-based service to create a tunnel)
  - automatic (deprecated, using IPv4 as low 32bits of IPv6)
    - ➢"6-over-4" (intra-domain, using IPv4 multicast as virtual LAN)
    - ➢"6-to-4" (inter-domain, using IPv4 addr as IPv6 site prefix)

59

Tunnel Brokers

- Operation
  - The user connects to a special web server (in the IPv4 network); makes tunnel application
  - The server assigns an IPv6 address, creates a DNS entry, informs the Tunnel Server, and sends a configuration script to the user
  - The user runs the script, installs the IPv6-over-IPv4 tunnel and connects to the Tunnel Server that routes the packets to the native IPv6 network

60

Automatic Tunneling Mechanisms:

6to4 Overview

- The most widely used mechanism
- In its basic configuration, 6to4 is used to connect two IPv6 islands across an IPv4 network
- Uses special 'trick' for the 2002::/16 IPv6 prefix that is reserved for 6to4 use
  - Next 32 bits of the prefix are the 32 bits of the IPv4 address of the 6to4 router
  - For example, a 6to4 router on 192.0.1.1 would use an IPv6 prefix of 2002:c000:0101::/48 for its site network

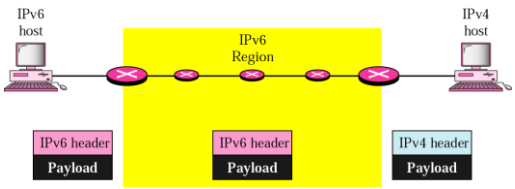
61

6to4 Contd..

- When a 6to4 router sees a packet with destination prefix 2002::/16, it knows to tunnel the packet in IPv4 towards the IPv4 address indicated in the next 32 bits
- Any site with single unicast IPv4 address can transmit to the IPv6 network using the 2002::/16 prefix

62

Header Translation



63

Header Translation

- Header Translation is necessary when majority of internet has moved to IPV6 but some still uses IPV4
- In this case header format must be totally changed through header translation
- The header of IPV6 is converted to IPV4
  - The job of the translator is to translate IPv6 packets into IPv4 packets by doing address and port translation and vice versa.

64

- This is a simple extension to NAT techniques, to translate header format as well as addresses
  - IPv6 nodes behind a translator get full IPv6 functionality when talking to other IPv6 nodes located anywhere
  - they get the normal (i.e., degraded) NAT functionality when talking to IPv4 devices

65

ICMP: Internet Control Message Protocol

- The purpose of ICMP messages is to provide feedback about problems in the IP network environment.
- ICMP Functions
  - To announce network errors
    - If a network, host, port is unreachable, ICMP Destination Unreachable Message is sent to the source host
  - To announce network congestion
    - When a router runs out of buffer queue space, ICMP Source Quench Message is sent to the source host
  - To assist troubleshooting
    - ICMP Echo Message is sent to a host to test if it is alive - used by *ping*
  - To announce timeouts
    - If a packet's TTL field drops to zero, ICMP Time Exceeded Message is sent to the source host - used by *trace route*

66

ICMPv6

- Two Types of ICMPV6 messages
- Error Messages
  - Destination Unreachable: cannot be forwarded to destination, port or address unreachable
  - Packet too big: when link MTU is smaller than size of packet
  - Time Exceeded: when hop limit becomes zero or exceeds in transit.
  - Parameter Problem : problem in any IP datagram field. eg., unrecognized next header field
- Informational Messages
  - Echo request: Sends request to any node to check reach ability
  - Echo reply: response from node for echo request

67

Network Traffic Analysis and Monitoring

- Process of capturing, decoding, and analyzing network traffic
  - Why is the network slow
  - What is the network traffic pattern
  - How is the traffic being shared between nodes
- Network Administrators are constantly striving to maintain smooth operation of their networks
  - need to monitor traffic movement
  - Need to monitor performance throughout the network and
  - verify that security breeches do not occur within the network.

68

Network Analyzer

- A combination of hardware and software tools what can detect, decode, and manipulate traffic on the network
  - Passive monitoring (detection) - Difficult to detect
  - Active (attack)
- Available both free and commercially
- Mainly software-based
- Also known as *sniffer*
  - A program that monitors the data traveling through the network *passively*

69

Who Uses Network Analyzers

- System administrators
  - Understand system problems and performance
- Malicious individuals (intruders)
  - Capture clear text data
  - Passively collect data on vulnerable protocols
    - FTP, POP3, IMAP, SMTP, HTTP, etc.
    - Capture VoIP data
  - Mapping the target network
  - Traffic pattern discovery
  - Actively break into the network (backdoor techniques)

70

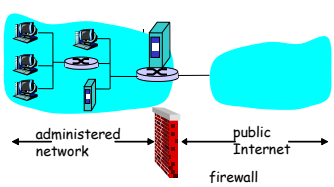
Firewall : Introduction

- Isolates organization's internal network from larger Internet, allowing some packets to pass, blocking others.
  - Acts as a security gateway between two networks
- A Firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.
- The use of single choke point simplifies security management because security capabilities are consolidate on a single system.
- A Firewall provides a location for monitoring security-related events.

71

Firewall Contd..

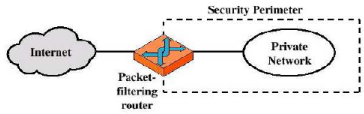
- Auditing and controlling access can implement alarms for abnormal behavior
- Windows Firewall helps protecting your computer by preventing unauthorized users from gaining access to your computer through a network or internet.



72

Firewall : Types of Firewall

1. Packet Filtering Router
   - It applies a set of rules to each incoming IP Packet.
   - The router is configured to filter packets going in both directions.
   - Router filters packet-by-packet, decision to forward/drop packet based on:
     - source IP address, destination IP address
     - TCP/UDP source and destination port numbers
     - ICMP message type
     - TCP SYN and ACK bits



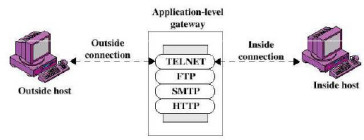
73

Packet Filtering Example

- Example 1: block incoming and outgoing datagram with IP protocol field = 17 and with either source or dest port = 23.
  - All incoming and outgoing UDP flows and telnet connections are blocked.
- Example 2: Block inbound TCP segments with ACK=0.
  - Prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

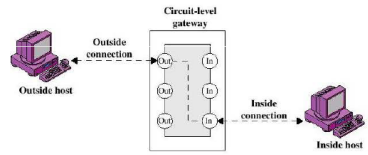
74

2. Application Level Gateway
   - They are called Proxy Servers and acts as a relay of application level traffic.
   - Example: allow selected internal users to telnet outside.
     1. Require all telnet users to telnet through gateway.
     2. For authorized users, gateway sets up telnet connection to destination host. Gateway relays data between 2 connections
     3. Router filter blocks all telnet connections not originating from gateway.



75

3. Circuit Level Gateway
   - It does not permit an end to end TCP Connection directly.
   - The gateway setups two TCP Connections (IN and OUT).
     - monitor TCP handshaking between packets to determine whether a requested session is legitimate
   - Once two connections are established => Gateway Relays



76

Firewall : Control Access Methods

1. Service Control
   - Filter traffic on the basis of IP address or TCP Port Address.
   - Example : Block Port 80, Allow Port 23
2. Direction Control
   - Determine the direction => Inbound/outbound.
3. User Control
   - Internal or External Users.
4. Behavior Control
   - Filter e-mail to eliminate Spam.

77

Limitations of firewalls and gateways

- IP spoofing: router can't know if data "really" comes from claimed source
- The firewall cannot protect against attacks that bypass the firewall.
  - Internal systems may have dial-out capability to connect to an ISP.
- The firewall does not protect against internal threats,
  - such as a dishonest employee
  - or an employee who unwittingly cooperates with an external attacker.
- The firewall cannot protect against the transfer of virus-infected programs or files.
- Impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, and messages for viruses.

78

Thank you!!!!