IT 4504
Section 7.0

Practical aspects of networking

Section 7.1

Structured cabling specifications and Standards

Industry Standards- (cabling for premises)

- Two sets of standards are widely used
  - EIA/TIA 658B
  - ISO/IEC 11801, the International Organization for Standardization standard

Industry Standards- (On Cables)

- CAT 5 and CAT 5e
  - Four pairs of AWG-24 solid cupper conductors .
  - Each pair is twist to reduce crosstalk.
  - 10BASE-T and 100BASE-TX using only two pairs
  - All four pairs are used in 1000BaseT mode
  - Operate at 100 MHz frequency .
  - Max length is 100m, practical distance is 90m
  - bend radius should be no less than 4 times the outer diameter of the cable

Industry Standards- (On Cables)

- CAT 6
  - Four pairs of AWG-22 solid cupper conductors .
  - Operate at 250 MHz frequency
  - Used for gigabit Ethernet and 10G networks
  - 55m for 10GBaseT networks.
  - bend radius should be no less than 4 times the outer diameter of the cable

Industry Standards- (On Cables)

- CAT 6a (Augmented Category 6)
  - Four pairs of AWG-22 solid cupper conductors .
  - Operate at 500 MHz frequency
  - Used for gigabit Ethernet and 10G networks
  - 100m for 10GBaseT networks.
  - bend radius should be no less than 4 times the outer diameter of the cable

Industry Standards- (On Cables)

- CAT 7and 7a
  - ISO standards for channel performance only
  - Speeds up to 1000Mhz allowing up to 100 Gbit/s
  - Category 7a is not recognized in TIA/EIA-568
  - Still at development stage.

TIA and ISO Equivalent Classifications

Frequency Bandwidth	TIA (Components)	TIA (Cabling)	ISO (Components)	ISO (Cabling)
1 - 100 MHz	Category 5e	Category 5e	Category 5e	Class D
1 - 250 MHz	Category 6	Category 6	Category 6	Class E
1 - 500 MHz	Category 6A	Category 6A	Category 6A	Class EA
1 - 600 MHz	n/s	n/s	Category 7	Class F
1 - 1,000 MHz	n/s	n/s	Category 7A	Class FA

Section 7.2

Network Security management

Firewalls

- A device or set of devices designed to permit or deny network transmissions based upon a set of rules.
- Divide to 4 basic types (generation)
  - First generation: packet filters.
    - work mainly on the first three layers of the OSI reference model.
    - Can filter on source or destination IP and port based rules
  - Second generation: application layer.
    - Works on all seven layers of the OSI model.
    - Can filter based on content.

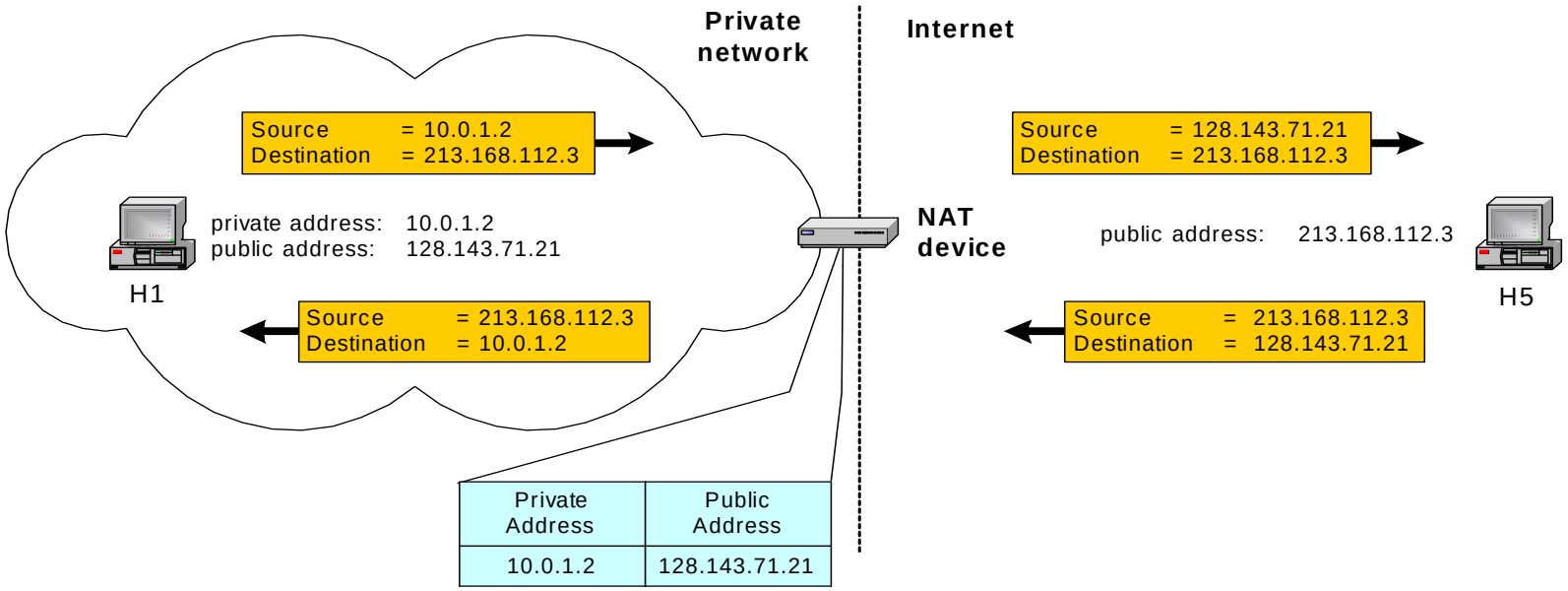
Firewalls

- Third generation: "stateful" filter.
  - Works on all seven layers of the OSI model.
  - Can filter based on content and keep track on the connection
- Forth generation :Dynamic Packet Filters .
  - Works similar to others but rules are modified on the fly.
  - This also called as active defense systems.

Network Address Translation (NAT)

- NAT is a router function where IP addresses (and possibly port numbers) of IP datagrams are replaced at the boundary of a private network
- NAT is a method that enables hosts on private networks to communicate with hosts on the Internet
- NAT is run on routers that connect private networks to the public Internet, to replace the IP address-port pair of an IP packet with another IP address-port pair.

Basic operation of NAT

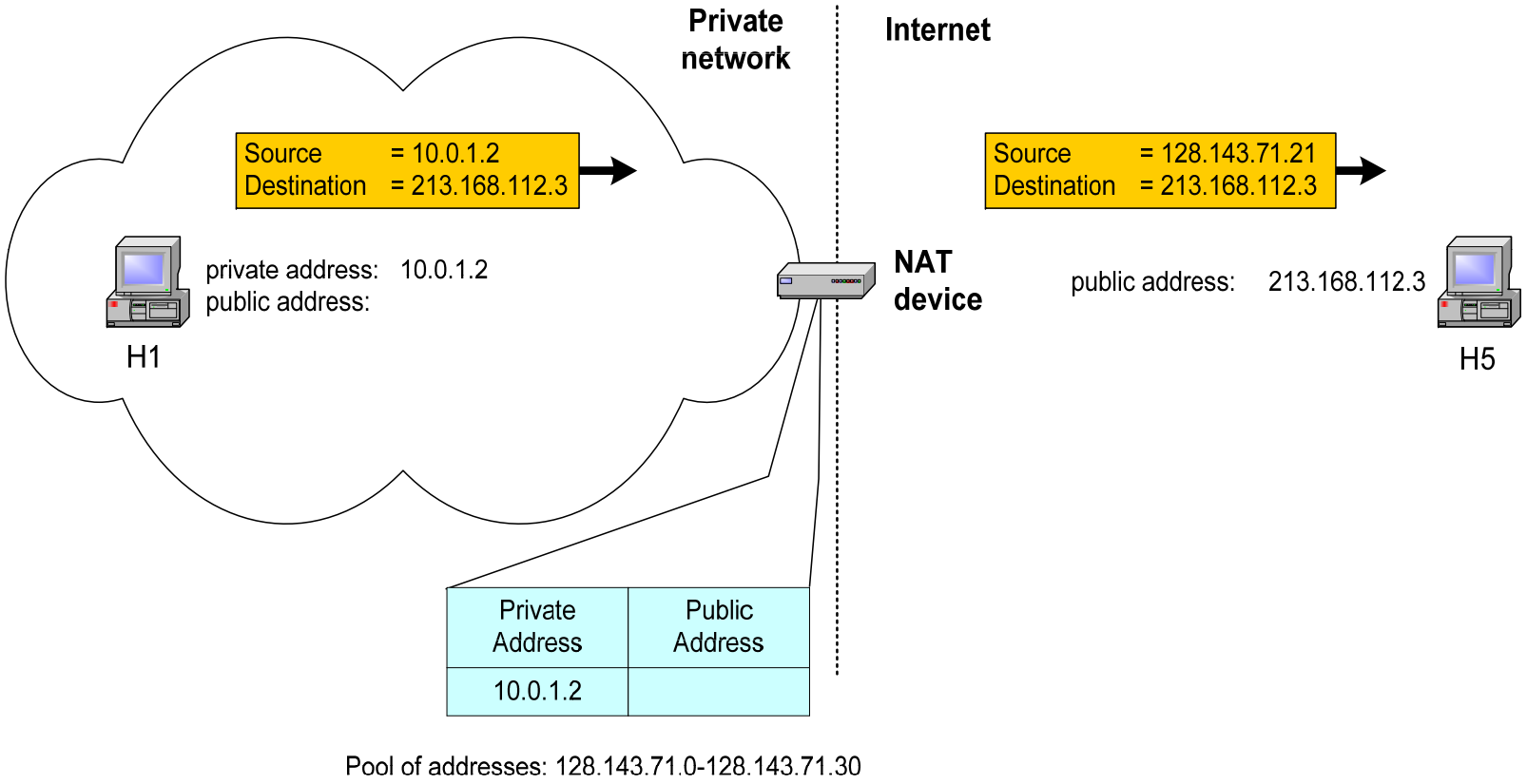


- NAT device has address translation table

Pooling of IP addresses

- **Scenario:** Corporate network has many hosts but only a small number of public IP addresses
- **NAT solution:**
  - Corporate network is managed with a private address space
  - NAT device, located at the boundary between the corporate network and the public Internet, manages a pool of public IP addresses
  - When a host from the corporate network sends an IP datagram to a host in the public Internet, the NAT device picks a public IP address from the address pool, and binds this address to the private address of the host

Pooling of IP addresses

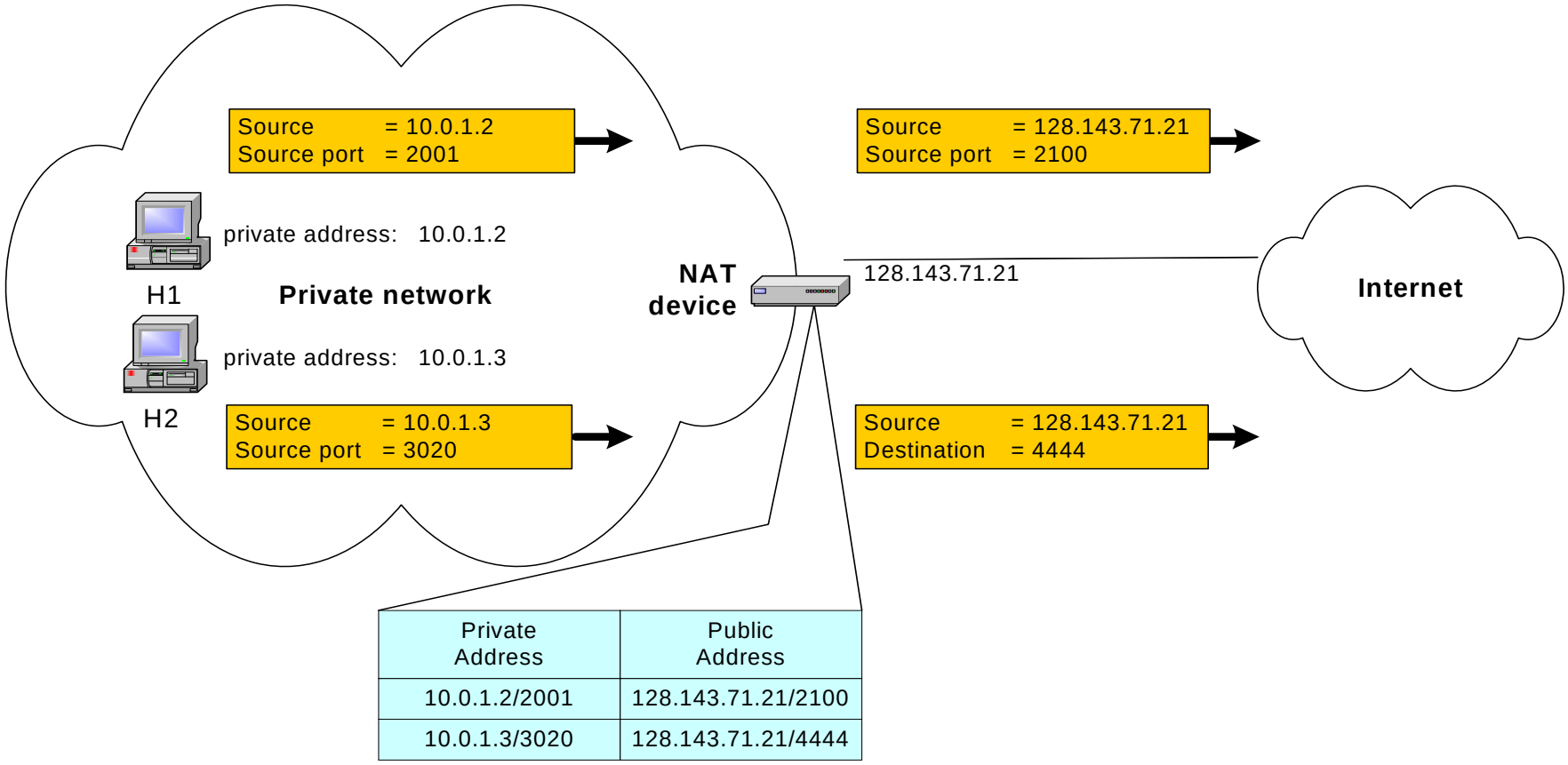


Pool of addresses: 128.143.71.0-128.143.71.30

IP masquerading

- **Also called: Network address and port translation (NAPT), port address translation (PAT).**
- **Scenario:** Single public IP address is mapped to multiple hosts in a private network.
- **NAT solution:**
  - Assign private addresses to the hosts of the corporate network
  - NAT device modifies the port numbers for outgoing traffic

IP masquerading

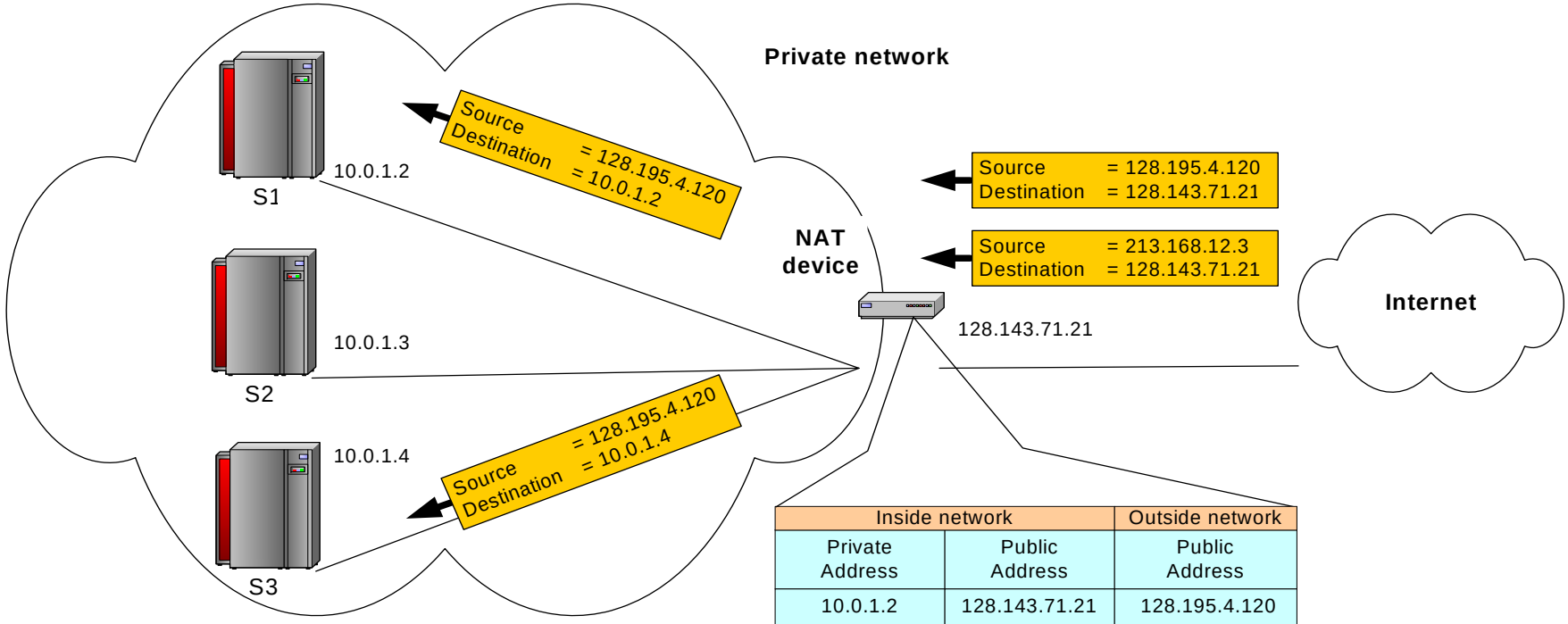


Private Address	Public Address
10.0.1.2/2001	128.143.71.21/2100
10.0.1.3/3020	128.143.71.21/4444

Load balancing of servers

- **Scenario:** Balance the load on a set of identical servers, which are accessible from a single IP address
- **NAT solution:**
  - Here, the servers are assigned private addresses
  - NAT device acts as a proxy for requests to the server from the public network
  - The NAT device changes the destination IP address of arriving packets to one of the private addresses for a server
  - A sensible strategy for balancing the load of the servers is to assign the addresses of the servers in a round-robin fashion.

Load balancing of servers



Inside network		Outside network
Private Address	Public Address	Public Address
10.0.1.2	128.143.71.21	128.195.4.120
10.0.1.4	128.143.71.21	213.168.12.3

Concerns about NAT

- **Performance:**
  - Modifying the IP header by changing the IP address requires that NAT boxes recalculate the IP header checksum
  - Modifying port number requires that NAT boxes recalculate TCP checksum
- **Fragmentation**
  - Care must be taken that a datagram that is fragmented before it reaches the NAT device, is not assigned a different IP address or different port numbers for each of the fragments.

Concerns about NAT

- **End-to-end connectivity:**
  - NAT destroys universal end-to-end reachability of hosts on the Internet.
  - A host in the public Internet often cannot initiate communication to a host in a private network.
  - The problem is worse, when two hosts that are in a private network need to communicate with each other.

Concerns about NAT

- **IP address in application data:**
  - Applications that carry IP addresses in the payload of the application data generally do not work across a private-public network boundary.
  - Some NAT devices inspect the payload of widely used application layer protocols and, if an IP address is detected in the application-layer header or the application payload, translate the address according to the address translation table.

Configuring NAT with iptable

- **First example:**

```
iptables –t nat –A POSTROUTING –s 10.0.1.2
          –j SNAT --to-source 128.143.71.21
```

- **Pooling of IP addresses:**

```
iptables –t nat –A POSTROUTING –s 10.0.1.0/24
          –j SNAT --to-source 128.128.71.0–
128.143.71.30
```

- **IP masquerading:**

```
iptables –t nat –A POSTROUTING –s 10.0.1.0/24
          –o eth1 –j MASQUERADE
```

- **Load balancing:**

```
iptables -t nat -A PREROUTING -i eth1 -j DNAT -
-to-destination 10.0.1.2-10.0.1.4
```

VLAN Implementation Benefits

- Improved Administration Efficiency
- Virtual Groups
- Reduction of Routing for Broadcast Containment
- Enhanced Network Security

Improved Administration Efficiency

- Moves, adds, and changes of workstations due to reorganization are one of the largest expenses relative to managing the network
- Vastly increased ability to manage dynamic networks and realize substantial cost savings due to VLAN
  - VLAN membership is not tied to a workstation's location in the network
  - When user's location changes, network address does not change

  - IP network
  - Router configuration remains intact

Virtual Groups

- Virtual group Model
  - Location dependent department/section
  - Dynamic organizational environment

    cross functional teams on a temporary project basis

- Managerial and architectural issues
  - Managing a virtual group
    - VLAN membership
  - Managing 80/20 group

Controlling Broadcast Activity

- Broadcast traffic can degrade network performance if not properly managed
- Broadcast firewall: Routers, VLAN
  - reduce overall broadcast traffic
  - minimize problems in one segment
- VLAN instead of routers
  - Higher performance and reduced latency
  - Ease of administration, Cost
    - ♦ Routers are more complex to configure
  - Cost

Enhanced Network Security

- LANs often have confidential, mission-critical data moving across them.
- Solution:
  - Segment the network into distinct broadcast groups by VLAN
  - Mainly true when VLANs are implemented with private port switching
  - Router access list when communicating between VLAN

Planning VLAN

- Defining LANs membership
- Best method for communicating VLAN membership information across multiple switches?
- Creating and differentiating workgroups
- Configuration automation
- Communication between different VLANs

How these issues are resolved determines the effectiveness of a particular VLAN implementation in meeting the needs of both users and network administrators

- By switch port group
  - Difficult to deal with user mobility
- By MAC address
  - Initialization of membership
- By network layer information (including by protocol type and/or IP address)
  - Longer time, virtual subnetwork
- By policy
  - More flexibility

Each method of defining VLAN membership has advantages and disadvantages.

Each method is appropriate for meeting different user needs and in different network environments.

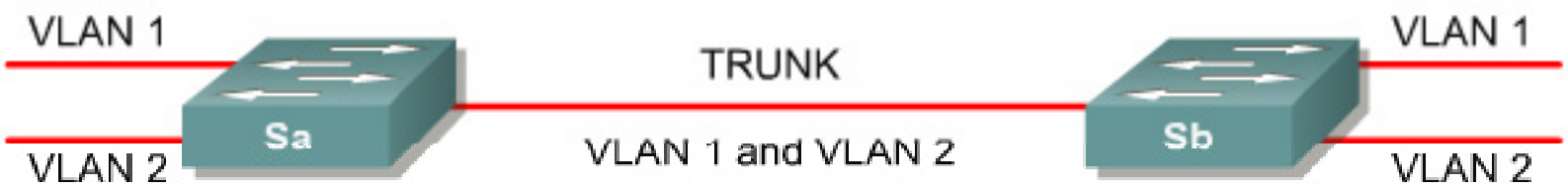
There are even situations where it is advantageous to utilize multiple methods within a single network environment.

VLAN Trunking Protocol

- **VLAN trunking:** many VLANs throughout an organization by adding special **tags** to frames to identify the VLAN to which they belong.
- This tagging allows many VLANs to be carried across a common backbone, or trunk.
- IEEE 802.1Q trunking protocol is the standard, widely implemented trunking protocol

VLAN Trunking

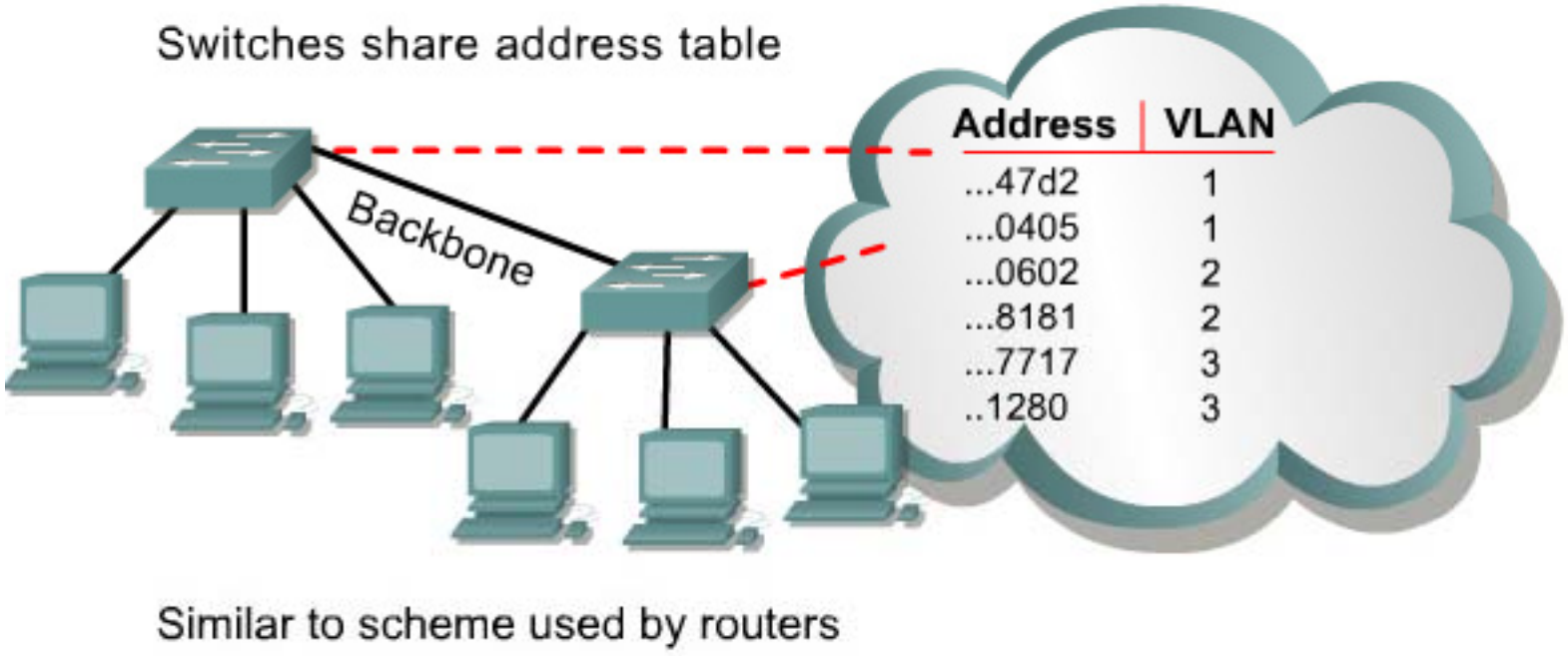
- Conserve ports when creating a link between two devices implementing VLANs
- Trunking will bundle multiple virtual links over one physical link by allowing the traffic for several VLANs to travel over a single cable between the switches.



Trunking Operation

- Manages the transfer of frames from different VLANs on a single physical line
- Trunking protocols establish agreement for the distribution of frames to the associated ports at both ends of the trunk
- Two mechanisms
  - frame filtering
  - frame tagging

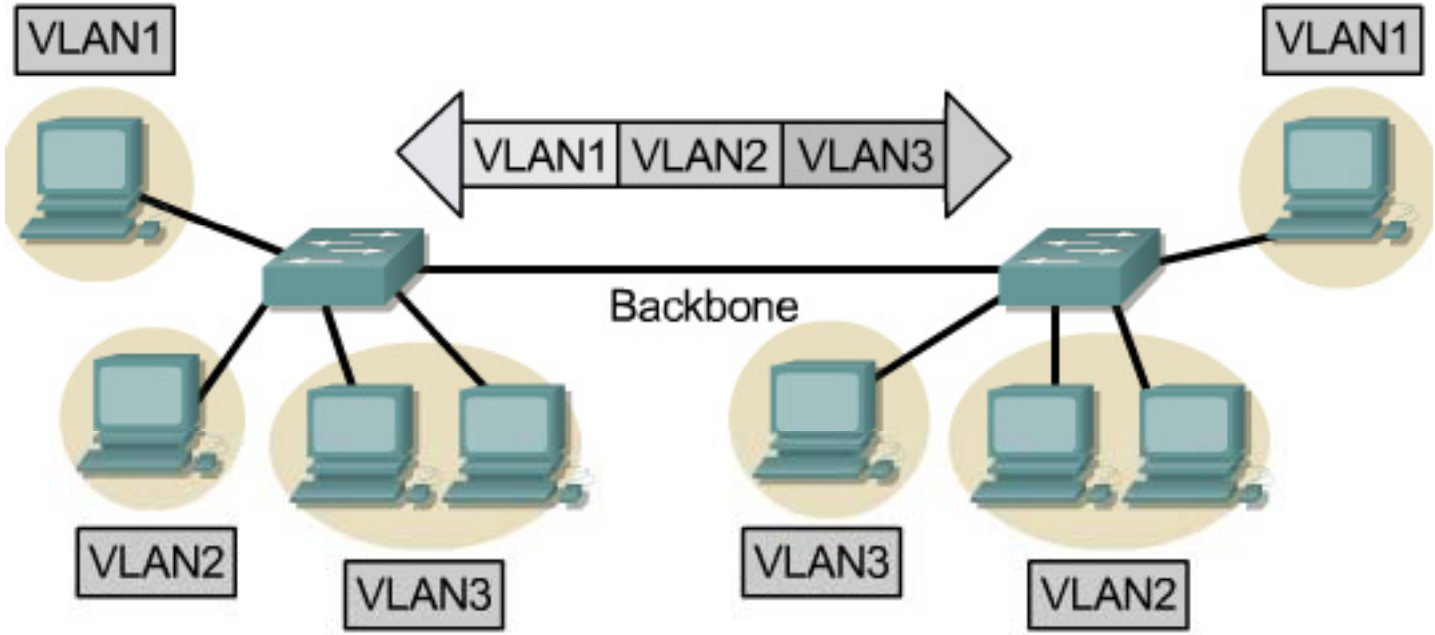
Frame Filtering



A filtering table is developed for each switch. Switches share address table information. Table entries are compared with the frames. Switch takes appropriate action.

Frame Tagging

- A frame tagging mechanism assigns an identifier, VLAN ID, to the frames
  - Easier management
  - Faster delivery of frames



Frame Tagging

- Each frame sent on the link is tagged to identify which VLAN it belongs to.
- Different tagging schemes exist
- Two common schemes for Ethernet frames
  - **802.1Q:** IEEE standard
    - Encapsulates packet in an additional 4-byte header
  - **ISL –** Cisco proprietary Inter-Switch Link protocol
    - Tagging occurs within the frame itself

VLANs and trunking

- VLAN frame tagging is an approach that has been specifically developed for switched communications.
- Frame tagging places a unique identifier in the header of each frame as it is forwarded throughout the network backbone.
- The identifier is understood and examined by each switch before any broadcasts or transmissions are made to other switches, routers, or end-station devices.
- When the frame exits the network backbone, the switch removes the identifier before the frame is transmitted to the target end station.
- Frame tagging functions at Layer 2 and requires little processing or administrative overhead.

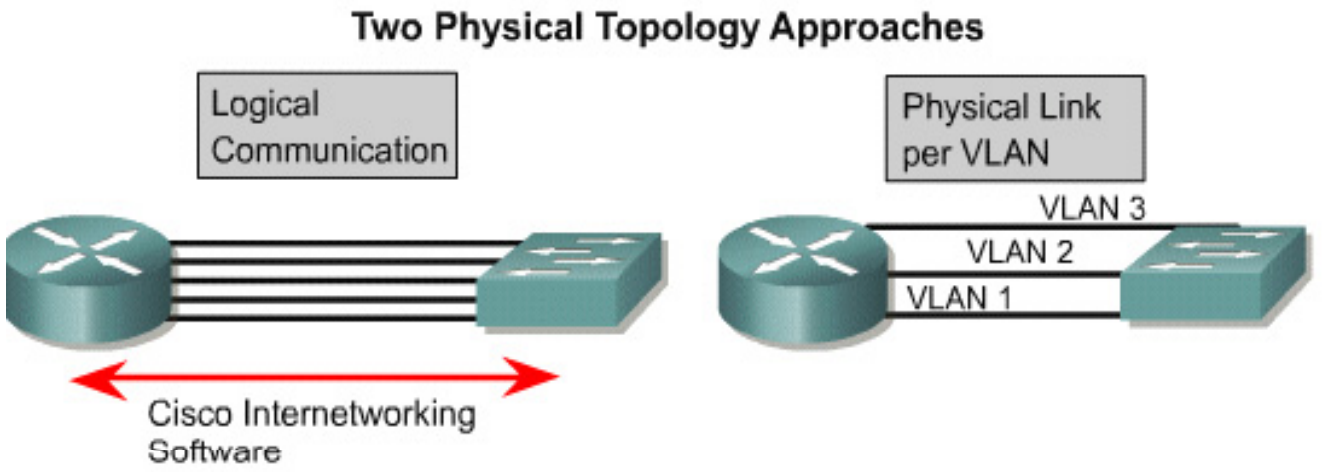
Inter-VLAN Routing

- If a VLAN spans across multiple devices a trunk is used to interconnect the devices.
- A trunk carries traffic for multiple VLANs.
- For example, a trunk can connect a switch to another switch, a switch to the inter-VLAN router, or a switch to a server with a special NIC installed that supports trunking.
- Remember that when a host on one VLAN wants to communicate with a host on another, a router must be involved.

Inter-VLAN Issues and Solutions

- Hosts on different VLANs must communicate
- Logical connectivity: a single connection, or trunk, from the switch to the router
  - That trunk can support multiple VLANs
  - This topology is called a router on a stick because there is a single connection to the router

Inter-VLAN Issues and Solutions (Contd.)



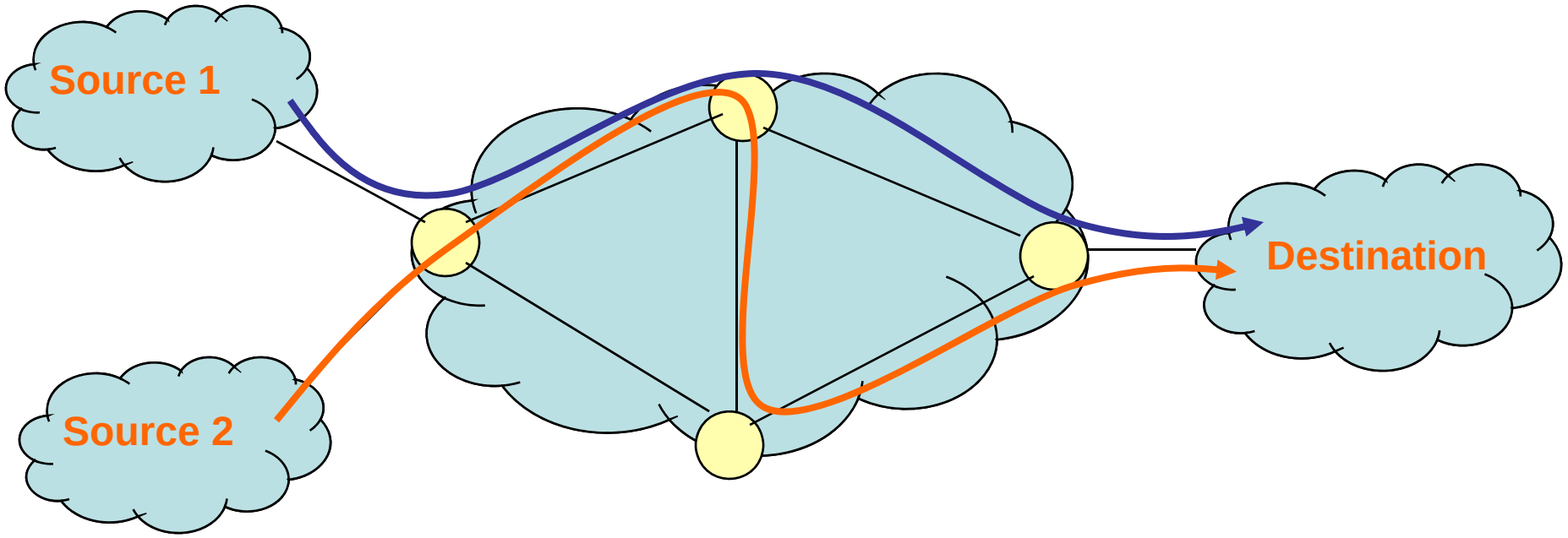
- Layer 3 router links VLANs together.
- Adds additional security and management.
- Logical links conserve physical ports.
- Multimode, depending on protocol.
- Controls access by VLAN.
- Up to 255 VLANs or greater per router

Why Tunnel?

- Security
  E.g., VPNs
- Flexibility
  - Topology
  - Protocol
- Bypassing local network engineers
  - Oppressive regimes: China, Pakistan, TS…
- Compatibility/Interoperability
- Dispersion/Logical grouping/Organization
- Reliability
  - Fast Reroute, Resilient Overlay Networks (Akamai SureRoute)
- Stability (“path pinning”)
  - E.g., for performance guarantees

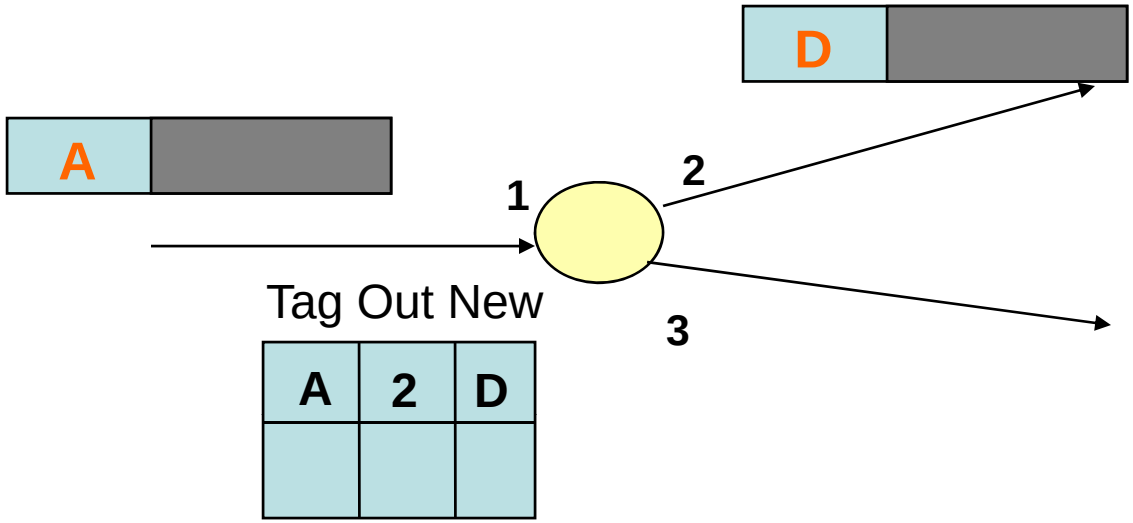
MPLS Overview

- **Main idea:** Virtual circuit
  - Packets forwarded based only on circuit identifier



Router can forward traffic to the same destination on different interfaces/paths.

Circuit Abstraction: Label Swapping



- **Label-switched paths (LSPs):** Paths are "named" by the label at the path's entry point
- At each hop, label determines:
  - **Outgoing interface**
  - **New label to attach**
- **Label distribution protocol:** responsible for disseminating signalling information

Layer 3 Virtual Private Networks

- **Private communications over a public network**
- A set of sites that are allowed to communicate with each other
- Defined by a set of administrative policies
  - determine both connectivity and QoS among sites
  - established by VPN customers
  - One way to implement: BGP/MPLS VPN mechanisms (RFC 2547)

Building Private Networks

- Separate physical network
  - Good security properties
  - Expensive!
- Secure VPNs
  - Encryption of entire network stack between endpoints
- Layer 2 Tunneling Protocol (L2TP)
  - "PPP over IP"
  - **No encryption**
- Layer 3 VPNs

Privacy and interconnectivity (not confidentiality, integrity, etc.)

Layer 2 vs. Layer 3 VPNs

- Layer 2 VPNs can carry traffic for many different protocols, whereas Layer 3 is “IP only”
- More complicated to provision a Layer 2 VPN
- Layer 3 VPNs: potentially more flexibility, fewer configuration headaches

Wireless Security?

- Hacking is no longer the esoteric domain of the techno-elite. Most often done by young people ages 15-25 that have extensive computer programming knowledge.
- Variety of reasons from simple curiosity all the way to achieving terrorist ideals.
- Most often used for identity theft and industrial espionage.

Capabilities

- Roaming Freedom
  - No longer constrained to the office
  - Smaller hand held devices have same functions as larger laptops/tablets
  - Never have to worry about access or “jacking-in”
- High Speed Data Transmission
  - Speeds may vary, but all are faster than dial up services
- Near Real Time Data Updates
  - Cases in SACWIS are updated when workers in the field get the information; decreases possible data loss due to memory errors

Wireless Networks

- Ensure all unused ports are closed
  - Any open ports must be justified
  - “Pessimistic” network view
- Enforce the rule of least access
- Ensure SSIDs are changed regularly
- Ensure insurance and authentication standards created and enforced

Encryption and Data Insurance

- USE STRONG ENCRYPTION!!
  - SHA-1 (Secure Hashing Algorithm)
- End to End Encryption
  - Initiate encryption at user and end at server that is behind the firewall, outside the DMZ
- ❑ Treat WLANs as untrusted networks that must operate inside the DMZ
- ❑ Access trusted network via VPN and two-factor authentication
- ❑ Increase application security
  - Possibly through use of an enterprise application system
  - Minimally through increased encryption

Encryption and Data Insurance

- Do not, under any circumstances, allow ad hoc WLANS
- Embrace and employ the 802.11i IEEE security standard
  - Native per user access control
  - Native strong authentication
  - (tokens, smartcards and certificates)
  - Native strong encryption
- Best bet for new wireless networks

Section 7.3

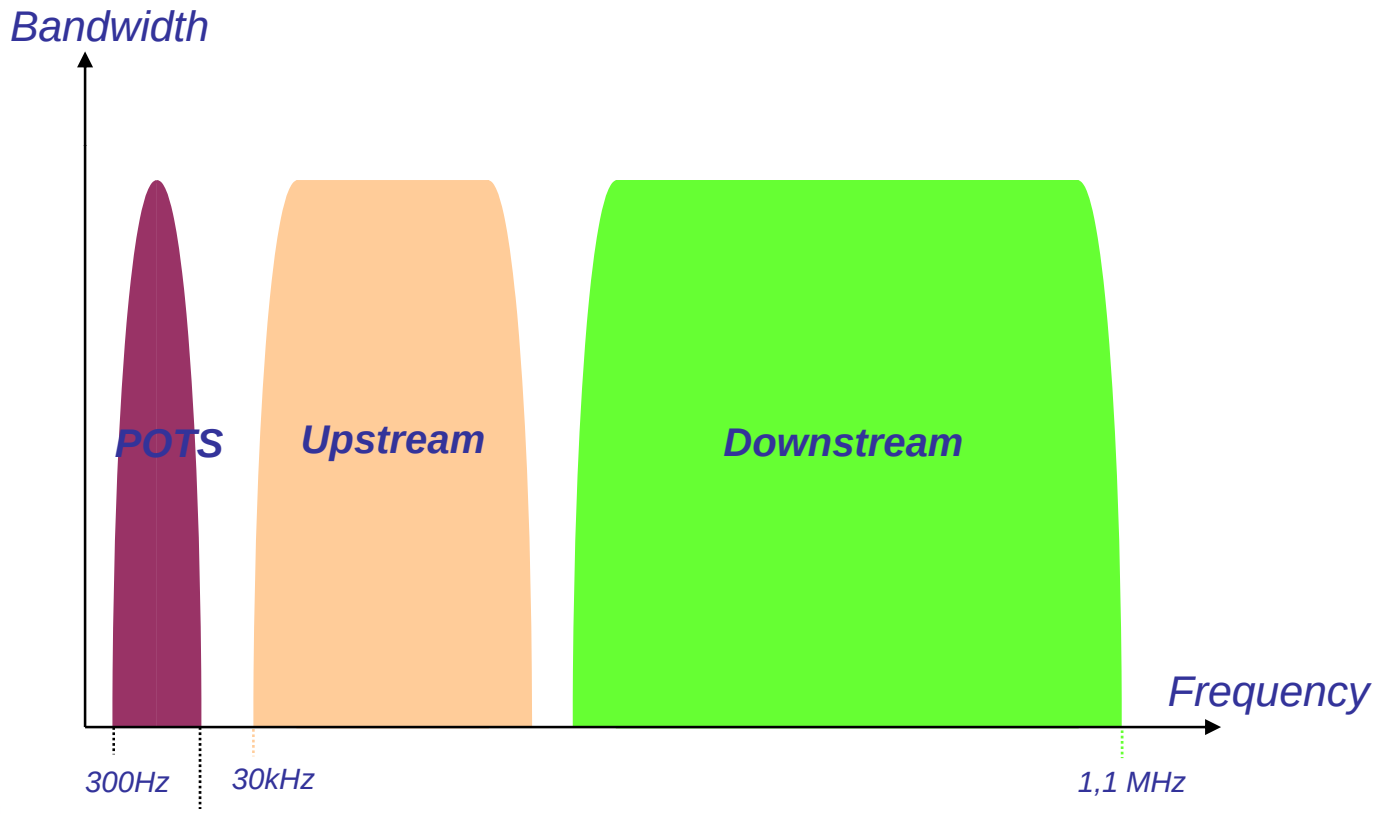
User access technologies

xDSL

- xDSL is the term for the Broadband Access technologies based on Digital Subscriber Line (DSL) technology.
- xDSL refers collectively to all types of digital subscriber lines, the main categories being ADSL, SDSL, HDSL, VDSL.
- DSL technologies use sophisticated modulation schemes to pack data onto copper wires. They are sometimes referred to as last-mile technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations.
- xDSL is similar to ISDN in like as both operate over existing copper telephone lines (POTS) and both require the short runs to a central telephone office (usually less than 5km).
- xDSL offers much higher speeds for upstream traffic, and downstream traffic and these streams can be either symmetric or asymmetric.

xDSL

- Frequency Division Multiplexing (FDM)
  - POTS, Upstream and Downstream Isolation



FTTH

- FTTH (fiber to the home) is a form of fiber optic communication delivery in which the optical signal reaches the end user's living or office space
- FTTH can be installed as a point-to-point architecture, or as a passive optical network (PON). The former requires that the provider have an optical receiver for each customer in the field. PON FTTH utilizes a central transceiver and splitter to accommodate up to 32 clients. Optical electric converters, or OECs, are used to convert the signals to interface with copper wiring where necessary.
- FTTH differs from Fiber To The Curb (FTTC) in that FTTC does not run directly to the home or building. Instead it runs to the curb, and the last leg of wiring to individual buildings remains copper wire.
- Fiber optic cables can currently carry information at speeds greater than 2.5 gigabits per second. Residential/business FTTH typically offers speeds from 10 mbps to over 100 mbps, which is a hundred times faster than most cable or DSL service.

GPRS

- General Packet Radio Service (GPRS) is a packet oriented Mobile Data Service available to users of Global System for Mobile Communications (GSM). It provides data rates from 56 up to 114 kbit/s.
- GPRS data transfer is typically charged per megabyte of traffic transferred, while data communication via traditional circuit switching is billed per minute of connection time, independent of whether the user actually is utilizing the capacity or is in an idle state.
- GPRS is a best-effort packet switched service, as opposed to circuit switching, where a certain Quality of Service (QoS) is guaranteed during the connection for non-mobile users.
- 2G cellular systems combined with GPRS is often described as "2.5G“
- It provides moderate speed data transfer, by using unused Time division multiple access (TDMA) channels in, for example, the GSM system.

EDGE

- Stands for Enhanced Data rates for GSM Evolution or Enhanced Data rates for Global Evolution
- Its and enhancement to 2.5G GPRS networks.
- A 3G technology .
- EDGE can carry a bandwidth up to 500 kbit/s (with end-to-end latency of less than 80 ms).

HSPDA

- High-Speed Downlink Packet Access (HSDPA) is a 3G (third generation) mobile telephony communications protocol in the High-Speed Packet Access (HSPA) family, which allows networks based on Universal Mobile Telecommunications System (UMTS) to have higher data transfer speeds and capacity.

- Current HSDPA deployments support down-link speeds of 1.8, 3.6, 7.2 and 14.4 Mbit/s. Further speed increases are available with HSPA+, which provides speeds of up to 42 Mbit/s downlink.

WiMAX

- Stands for Worldwide Interoperability for Microwave Access.
- A technology use for last mile wireless broadband access as an alternative to cable and DSL, xDSL.
- IEEE 802.16 standard is for 'WiMAX‘
- WiMAX Release 1 based on IEEE 802.16e technology.
- The P802.16m define speeds up to 100 Mbit/s mobile & 1 Gbit/s fixed units and refers as WiMAX Release 2
- no uniform global licensed spectrum for WiMAX
- IMT-2000 specify global spectrum as 2.5 GHz, 2.69 GHz for IMT-2000 recognized countries.
- WiBro developed by the South Korean telecoms industry based on IEEE 802.16e -mobile WiMAX

End of Section 7.0