ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Τεχνολογίες Τηλεπικοινωνιών και Δικτύων
κ. Οικονομίδης
κ. Πομπόρτσης

Core / Backbone Networks

Παπανικολάου Γιάννης - Α.Μ. 05/34

Φεβρουάριος 2006

INDEX

1. NETWORKS: STATE OF THE ART (Abstraction).....5
1.1. B-ISDN, OSI, TCP/IP models 5
1.2. Data, control and management..... ..6
1.3. Network organization, foundation and development..... 7
1.4. Core and access networks 8
1.4.1. Access networks.....9
1.4.2. Core networks 9
1.5. Networks topologies.....11
1.6. Transmission media and devices.....12
1.6.1 Media..... 12
1.6.2 Devices 14
1.7. Backbone Architectures..... 15
1.7.1 Backbone Architecture Layers.....15
1.7.2 Backbone Network Types..... 15
1.8. Communication transmission means..... 22
1.8.1. T1 and T3 22
1.8.2. SONET.....22
1.8.3. ATM networks 22
1.8.4. IP networks.....23
1.9 Economy of networking business 23
1.10. Network requirements evolution 23
1.10.1. Internet development.....23
1.10.2. Side-effects.....24
1.10.3. Present networks requirements 25

2. Planning and Designing Principles
2.1. Planning Strategy.....27
2.2. Location Planning.....27
2.3. Network Design and Routing.....28
2.4. Failures and Routing Convergence.....29
2.5. Network Design in Practice.....29
2.6. Bandwidth Management.....30
2.7. Quality of service.....30

3. Traffic Engineering.....33
3.1. Network vs. traffic engineering.....33
3.2. TE definition.....34

3.3. ATM (Asynchronous Transfer Mode) 34
3.4. Gigabit Ethernet.....36
3.5. 10-Gigabit Ethernet.....37
3.6. MPLS (Multiprotocol Label Switching) 38
3.7. SONET (Synchronous Optical Network) and WDM
(Wavelength Division Multiplexing) 39

Appendix.....44

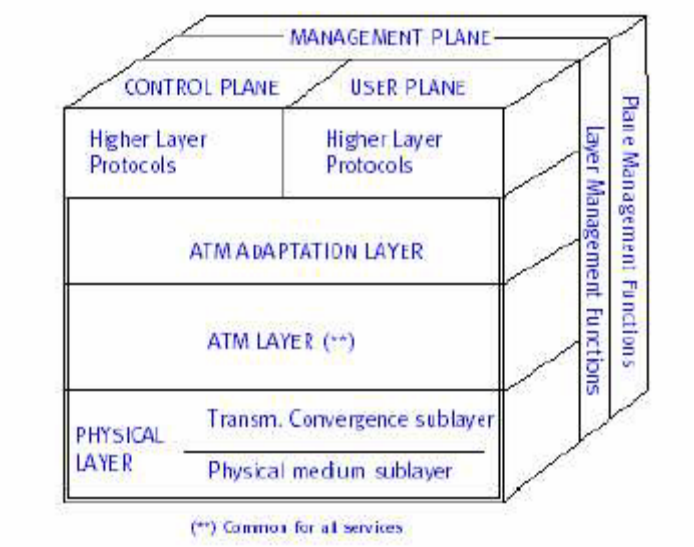
1. Networks: state of the art (Abstraction)

Main objective of the project is to introduce key concepts and the status of networks. The view on the current and emerging network development reveals problems and requirements for networking technologies.

Communications and networking areas encompass multitude of conceptual domains that can be perceived from different multi-dimensional perspectives. There can be two worlds distinguished in the field - the one of standards and another of real industry implementations. This project focuses mostly on the standards that create framework for the universal knowledge and understanding of network concepts.

1.1. B-ISDN, OSI, TCP/IP models

The most common standard networking model representation comes from ITU-T_I.371. B-ISDN protocol reference model [I.371] and is illustrated as layer architecture with attached perpendicular planes



ITU-T I.371 B-ISDN reference model

Regarding layered abstraction, traditionally OSI reference model is exposed. It reflects architecture of operational principles. E.g. layering idea indicates the division in terms of designed purposes and

applications. It has been developed as a conceptual abstraction to help develop framework for protocols for Open Systems Interconnections.

There is also TCP/IP model that has been developed as a more practical view, specially suited for IP-based systems.

Table 1.1.OSI and TCP/IP reference models

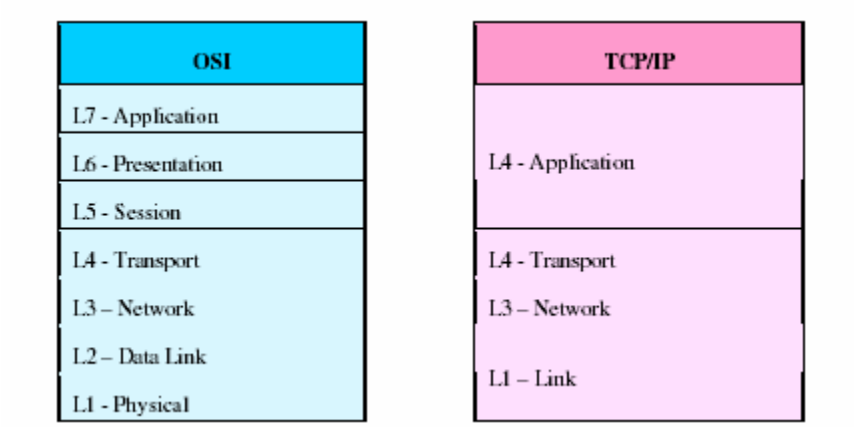


Table 1.1 presents OSI and TCP/IP models with referenced layers.

There are cases where neither OSI nor TCP/IP models associate functionality with protocols directly. E.g. routing protocols, typically functionally associated with OSI L3 (routers are claimed to possess L3 functionality), operate at higher layers in fact. Thus, OSI model refers to functional external view – not precisely the internal operation. The protocol stack pictures the operational inter-relations and dependencies.

1.2. Data, control and management

Another abstraction [NGNI-D4] involves the plane structure concerning data, control and management. This view can be treated as another dimension or perspective regarding division in terms of network functionality. It is seen in another dimension than OSI model. To clear the concepts, it is worth to mention that data plane (also referred as user transport plane) provides transport of raw user information (e.g. can be implemented in ASIC hardware) along with associated flow and congestion control (e.g. buffering and shaping).

Control plane involves control capabilities and is responsible for routing, path control and/or connection control, signalling and protection functions. E.g. In a simplified view, routing protocols are

used for control features, whereas forwarding is done by hardware on basis of consulted forwarding table, determining next-hop.

Management plane is responsible for coordinating functionalities with regards to planes as well as protocols, parameters and resources. Management procedures, opposed to control practices, are engaged for a long term and involve static provisioning and device configuration, monitoring, fault management and restoration.

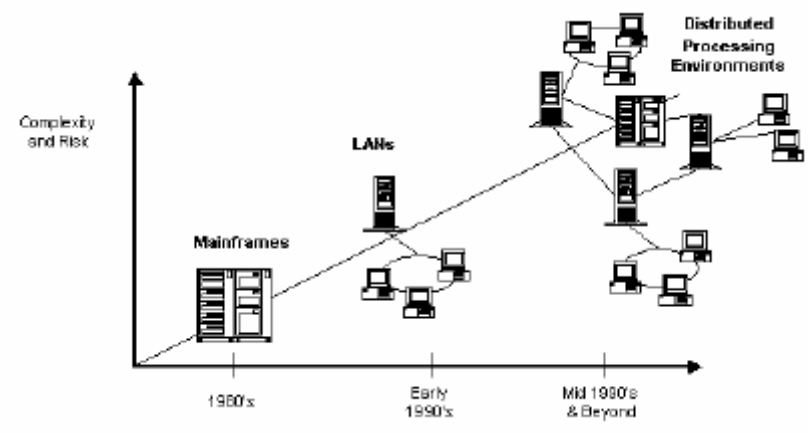
1.3. Network organization, foundation and development

The shape of current networks has been formed over time reflecting the evolution of communication needs accompanied by technological advances. The more and more demands arise for products and services such as information exchange and distribution through various public and private networks. New models of work management take course towards distributed approach where cooperation and information sharing contribute to the success. Virtual private networks (VPNs), corporate intranets, global extranets are commonly employed worldwide.

Welcoming affable and cheap access technologies, such as digital subscriber line (DSL), encourage rapid expansion of digital society. Indeed, the greater the network scope the more advantageous it becomes to join the global system. Technological advances act as catalysts creating demands for more sophisticated services such as advanced e-commerce-based solutions, real-time audio and video, voice over IP (VoIP) and video conferencing. Their implementation stipulates different requirements from the network in terms of reliability, accuracy, and delay or information volume.

Future services - connected anywhere anytime [OCAA]

Various divergent communications means within computer-, telephone- and television- domains are becoming coexisting within one networking realm. Future requirements head toward anywhere anytime connectivity challenges. The Internet rapid development has driven dramatic increase of data traffic. It is forecasted to keep the increasing rate, surpassing largely voice traffic level. The great diversity of applications and services present in the digital world pleas for convergence. The network environment evolution is presented in following Figure.

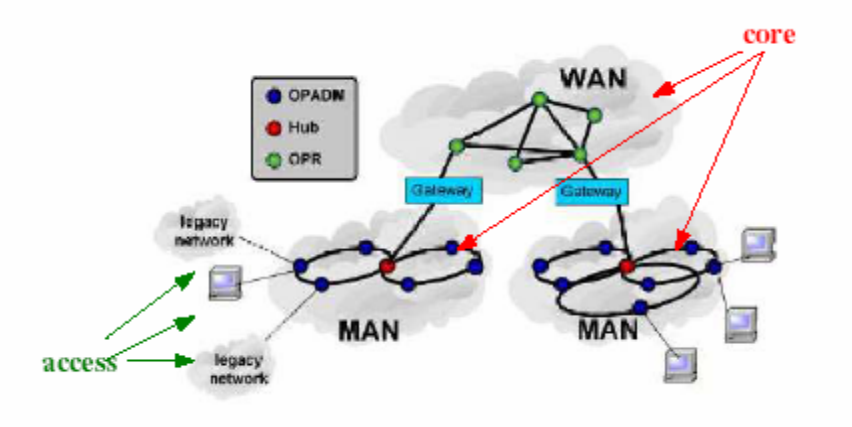


Network environment evolution

The increasing demand for communication services is one of the main drivers for efficient broadband technologies.

1.4. Core and access networks

The network architecture has been shaped over time and developed to face the evolving communication requirements. There can be numerous approaches for network design but always some general rules exist that make the network form an organized architecture. When looking at physical structure a general model can be recognized as example:



There are two structural differences that divide the network into core and access parts. The design differences come from the divergent requirements and roles the component networks are supposed to play. Also, networks can be divided with respect to their scope into:

LANs – Local Area Networks,
MANs – Metropolitan Area Networks,
WANs – Wide Area Networks

1.4.1 Access networks

Access network, referred also as the local loop, presents an "interface" for connecting users or customers to the backbone network. The old days telephony terminology denotes access networks the last drop. The design of access network usually focuses on users demands for providing end quality for their communication services. The requirements for access networks are quite precise and thus, the design and capacity planning can be more accurately suited to the actual needs and is more moderate in scope and cost. Besides, access networks change in shape quite dynamically. The planning is done in the way so that when new users are added usually the network needs to be easily adjustable. It is easy to obtain cost effective solution when relevant design is applied so that the costs are reasonably shared by accounted number of users.

1.4.2 Core / Backbone networks

Core network forms a central 'spine' and is usually referred as the backbone or trunk network. The backbone networks are characterized with high-capacity network infrastructure designed to

accommodate multiple traffic streams from numerous access networks and also aimed to face their low latency objectives.

They provide transport service for huge number of users that results in enormous demands for huge bandwidth. Also, they should provide high level of resilience as failure of the core may affect all users.[4]

The backbone network is an important architectural element for building enterprise networks. It provides a path for the exchange of information between different LANs or subnetworks. A backbone can tie together diverse networks in the same building, in different buildings in a campus environment, or over wide areas. Generally, the backbone's capacity is greater than the networks connected to it.

There are *distributed backbones* that snake throughout a building or campus to provide a connection point for LANs, and there are *collapsed backbones* that exist as wiring hubs and switches. A hybrid configuration ties together several collapsed backbone hubs or switches with a distributed backbone.

A backbone is typically a network that interconnects other networks. In a switched network design, a backbone is not as clearly defined. It is usually just the high-speed switches that aggregates traffic from attached networks. [2]

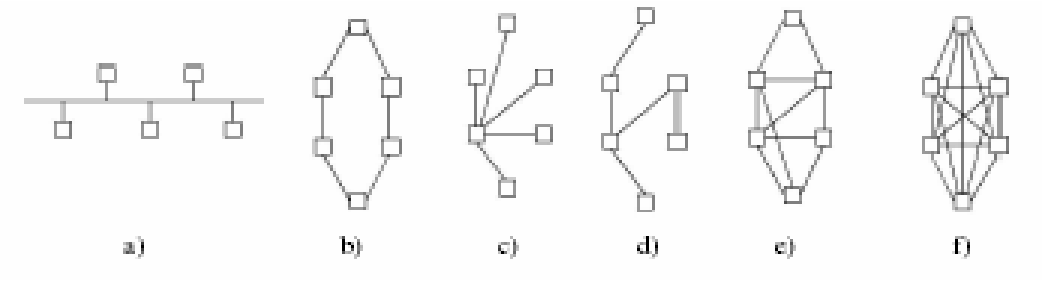
The core network planning requires more anticipation and long term perspectives to be considered. The design needs to account for varying number of customers and their communication demands and resulting changing traffic patterns. The topology should be kept stable – adding new nodes should be avoided - instead the nodes and circuits should be easily upgradeable.

Core networks usually provide transport service for access networks. The customers issue their quality requirements for end-to-end communication and it is the core that has to guarantee their traffic treatment according to approved service level agreements (SLAs). Core networks usually support multiple services, which means that various classes of service share the transmission, switching, management, and other resources of the network. Thus, the backbone network planning and management practices require appropriate strategy to prepare relevant and reliable environment for their clients.

As the project is devoted to core networks, the subjects dealt in the report regard the backbone network issues. The greatest and most evident core network is the Internet. However, its structure is very heterogeneous in nature and should not be generalized as one network matter. Generally the Internet can be treated as one major general core with composition of network islands considered as secondary backbones operated as proprietary internetworks. [4]

1.5. Networks topologies

There are different approaches for setting up network infrastructure. The way of connecting devices is usually seen as topology. Topologies may involve: bus, ring, star, tree, (partial or full) mesh, hybrid schemes. Their models are presented in following Figure.



Network topologies:
a) bus, b) ring, c) star, d) tree, e) partial mesh, f) full mesh

Except for bus structure, the rest of topologies could be used within WANs.

Bus networks are deployed in LANs, usually connected with Ethernet coaxial cables. They are no resilient to failures.
Ring topologies are commonly used within MANs and WANs e.g. Token Ring technology or modern transmission systems. They can provide efficient resilience against single-failures.
Star network can be found mostly within LANs. The scheme may be also used for connecting terminals to central site within wide-areas as well. However, generally the star networks are not resilient to failures.
Tree networks can provide setup for connecting terminals to cluster controllers at intermediate site and the mainframe site, typically implemented over WANs. They do not provide resiliency but can minimize shorter circuits costs.
Mesh networks can become more costly, involving multitude of nodes and links. Nevertheless, they are very resilient even to multiple

failures, depending on the mesh density. They are implemented in WAN environments.

In practice there are also multiple hybrid solutions implemented. **Within cores**, the most common structures resemble ring and mesh network or some combined approach.[4]

1.6. Transmission Media and Devices

1.6.1 Media

To start we need to understand the medium that comprises the network and links to the network backbone.

The medium is really a fancy way of saying cabling. There are three very basic mediums to choose from, each with advantages and disadvantages. The three are Coaxial Cable, Twisted Pair, and Fiber. A Fourth also exists WIRELESS but when it comes to the corporate infrastructure and backbone, Wireless just isn't as prevalent. Each is a great medium in its own right but each with very distinct features.

Coaxial Cabling (Coax)

Coaxial Cabling (Coax) is one of the oldest of the mediums. It consists of a copper wire surrounded by a cladding and a wire mesh wrapping encased in sheath. It is used today largely for cable TV and cable modem (which by the way is nothing more than a huge fancy network) carriers. It is one that most people are familiar with. It provides good EMI (electromagnetic interference) protection and offers great signal strength over a distance. It is highly flexible and low in cost. But how prevalent is it in today's corporate networking infrastructure? Not as prevalent as it once was. One of the chief disadvantages of this type of cabling is that it lends itself to very linear networking (bus topologies). Not a lot of companies deal with this type of networking much anymore. You had to tie computers together using T connectors and special nic's that had a coax connector on it, which are difficult to find. Each bus had to be terminated properly or signaling would be problematic. Troubleshooting a failed terminator is one of those special joys in life that everyone should have to deal with.

Twisted Pair

The most popular of the mediums today in the corporate

infrastructure is Twisted Pair. Twisted pair comes in many different flavors such as, shielded or unshielded, Plenum or Non-Plenum, and Solid or Stranded. There are many different categories to choose from. CAT3 (primarily used for standard POTS and 10Mb Ethernet), CAT5 (typical 10/100 Ethernet), CAT5e (typical 10/100/1000 Ethernet), CAT6 (typical 10/100/1000 Ethernet and Short Distance 10GB Ethernet), and Modified CAT6/CAT7 (802.3an 10GB Ethernet Long Distance). The cost on Twisted Pair is relatively inexpensive and supports your standard RJ45 connector most of us are familiar with. Most of the networking devices built support this kind of cabling. **But what are the benefits and drawbacks**? The main benefits are that people are most familiar with it, it is easy to work with and modify, and it has decent distance. The biggest drawback really is it is more susceptible to EMI than the other two mediums and distance is limited to 100 Meters unless a signal repeater is used (the longer the run the more susceptible the signal is to attenuation).

Fiber Optic

The third medium is Fiber Optic Cabling. It also comes in many different flavors Plastic Vs Glass, Loose Tube vs. Tight Buffered, and Multi Mode Vs Single Mode. It also comes in many different thicknesses such as 8.3 Microns, 10 Microns, 50 Microns, 62.5 Microns, and 100 Microns. The most common of the fiber installations used in corporate infrastructures is a 62.5 Micron Core Multi-Mode Fiber Optic Cable. The benefit to fiber is that it can be used over exceptionally long distances and it suffers no EMI/RFI. The drawback is the cost. The type of cable though is determined by the equipment being used, LED (Light Emitting Diode) vs. ILD (Injection Laser Diode). Either way you slice it Fiber is the best but the most costly.

Wireless

The final medium is wireless. Their have been some big advancements in wireless technology but it is not the preferred medium for a network, especially not on a backbone. It has some very big advantages, such as a workstation can be moved from place to place without having to worry about the cabling, it is fairly fast (still not as fast as a traditional wired network but getting their), and allows for a lot of flexibility. However, there are some very serious drawbacks. Security is one of the biggest overheads on a wireless network. It has an intrinsic need to be locked down at each AP. It also has no real boundaries, which can be difficult if the network has been locked down. Also, devices don't always interoperate properly (try

using a Symbol AP with a Aironet Wireless card some time) because all manufacturers have not agreed on some of the standards. Another thing is that it can be spoofed easier allowing for a rouge device to penetrate the network. Finally, there is Bluetooth, which gives the ability to ad hoc, which is both an advantage and disadvantage.

1.6.2 Devices

The devices that are used in the Network that utilize these mediums are Hubs, Switches, Routers, AP's, and Bridges.

Hubs

Hubs come in different speeds (10/100/1000), generally broadcast a signal to all of the ports, the bandwidth is shared by all connections, and the cost is relatively inexpensive. Hubs ability is very limited because it must negotiate a connection to the lowest common connection for all ports.

Switches

Switches (Intelligent Hubs) on the other hand, also come in different speeds (10/100/1000/10GB) but unlike Hubs, each port's bandwidth is dedicated, it can be segregated into VLAN's, and Broadcast's can be limited. The numbers of features it can support are determined by the cost. Also Switches can be purchased to work on different Layers of the OSI. The higher the layer is supports the more costly the switching device is. A typical switch is only a layer two device, however, a layer three switch can act as a router and layer 4-7 switches can act as a router plus added things like SSL Acceleration.

Routers

Routers are complex devices and are used for connecting disparate systems and devices. Routers are also used in segregation of differing LANS, MANS, and WANS. They are have a table of varying routes and perform routing functions and calculations. They also can have a filtering mechanism to disallow certain protocols and help limit unwanted communications. These devices are generally very costly and take a very thorough understanding of networking functions both on LANS, MANS, and WANS (Which includes the internet). Routers can also perform some bridging functions.

AP's - access points

AP's (access points) are used in a wireless scenario. It gives the ability to act as a router, a repeater, or both. It also has some switching abilities built in, as well as, some security controls. It is not necessary to have AP's in a wireless network. Unfortunately without them the range is very limited and the number of devices that can participate is also limited. AP's function as a security control (example: MAC Address Restricted AP's attempt to limit a machines ability to attach to a network [But MAC's can and have been Spoofed]), a repeater (to extend signal range), and possibly as a router. Also AP's will need to be used if multiple floors are involved to enable end-to-end communication throughout the infrastructure. To be completely cutting edge, wireless networks can be linked using satellite or microwave dishes in a CAN, MAN, or WAN Scenario.

Bridges

Bridges are used primarily to link different types of topologies within a network. For example, A Bridge is used to allow a Token Ring LAN to communicate with an Ethernet LAN. Utilizing some server software's and multiple types of NICS within a Server can also accomplish bridging. [3]

1.7. Backbone Architectures

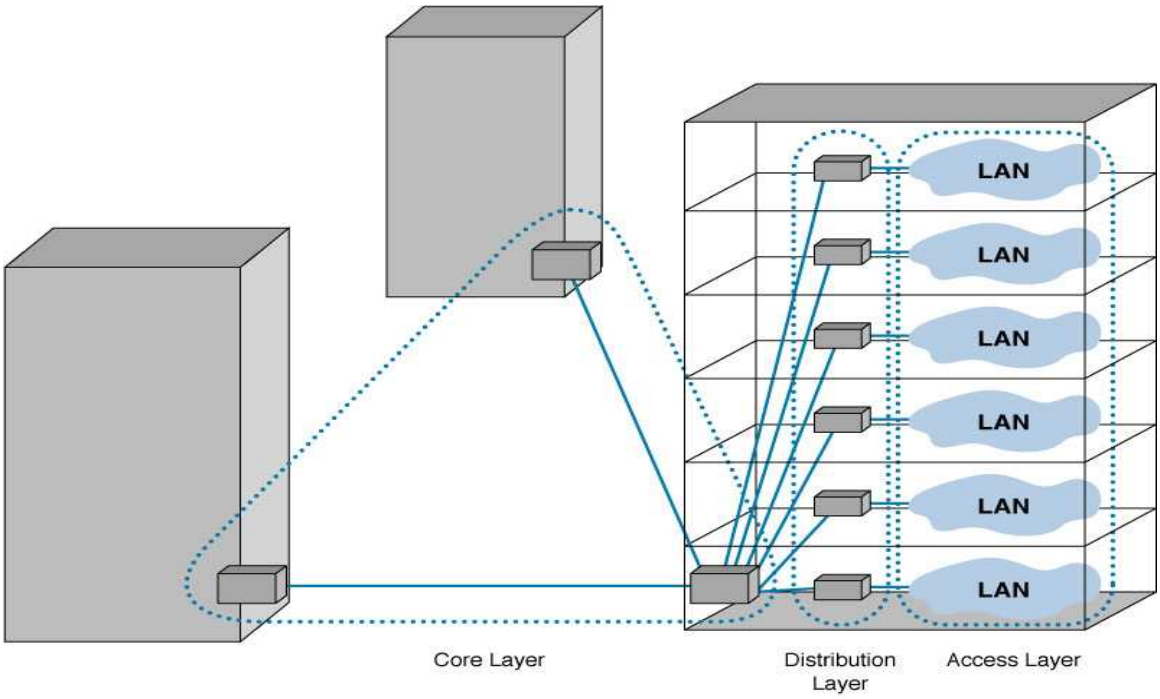
1.7.1 Backbone Architecture Layers

- Network designs are made up of three technology layers:
- The **access layer** which is the technology used in LANs
- The **distribution layer** connects LANs together
- The **core layer** connects different backbone networks together

1.7.2 Backbone Network Types

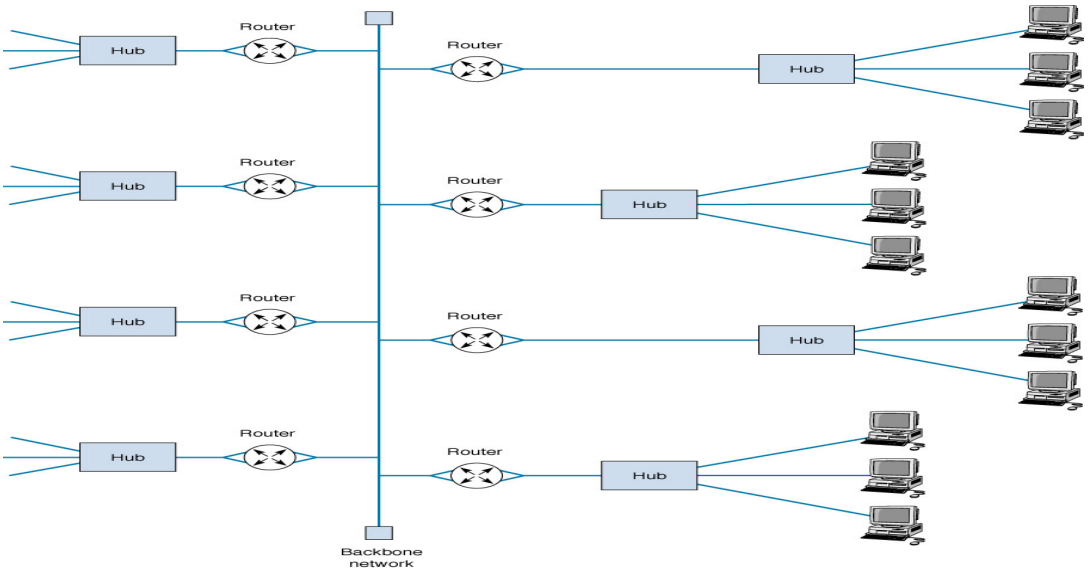
There are four basic types of backbone networks:

- Routed Backbones
- Bridged Backbones
- Collapsed Backbones
- Virtual LANs



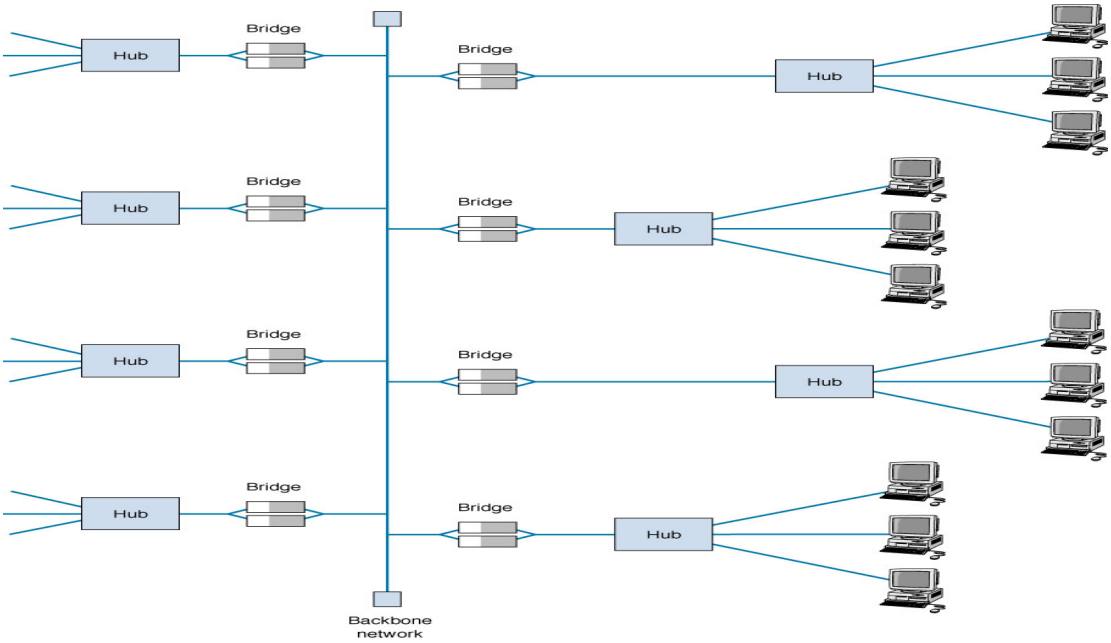
Routed Backbones

- Routed backbones move packets using network layer addresses, typically using a bus topology.
- Each LAN is a separate and isolated network.
- LANs can use different data link layer protocols.
- Main advantage: LAN segmentation.
- Main disadvantages:
  - routers tend to impose time delays compared to bridging and (layer 2) switching
  - routers require more mgmt. than bridges & switches.



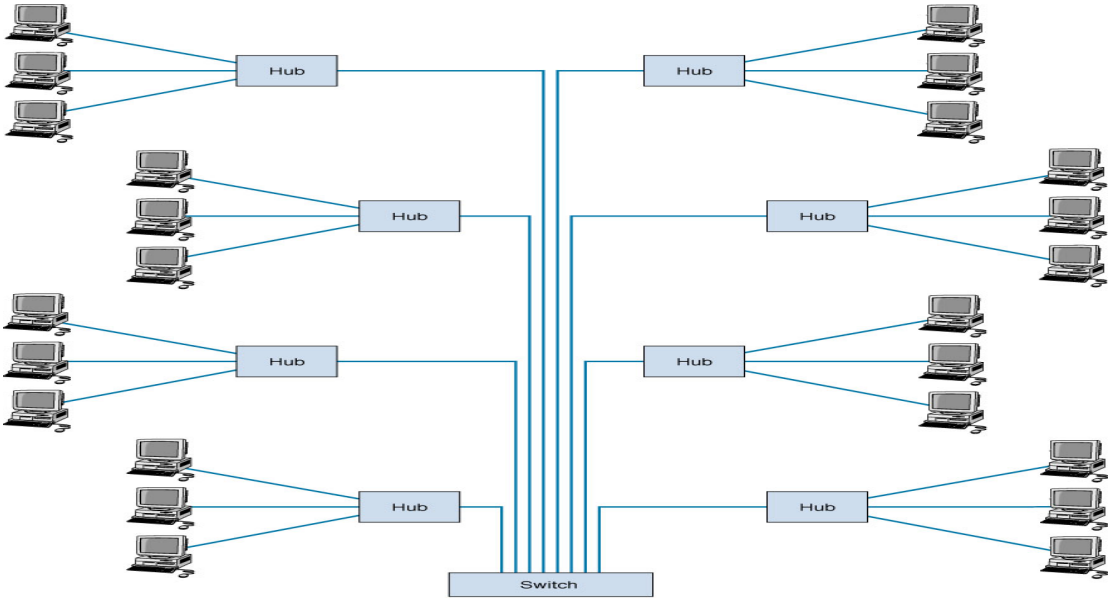
Bridged Backbones

- Bridged backbones move packets between networks using a bus topology, forwarding of packet is based on their data link layer addresses.
- The entire bridged backbone network forms just one subnet.
- Formerly common in the distribution layer, their use is declining due to performance problems.
- Bridged backbones are cheaper (since bridges are cheaper than routers) and easier to manage than routed backbones.
- For small networks, a bridged backbone performs well, but for large networks broadcast messages can lower performance.



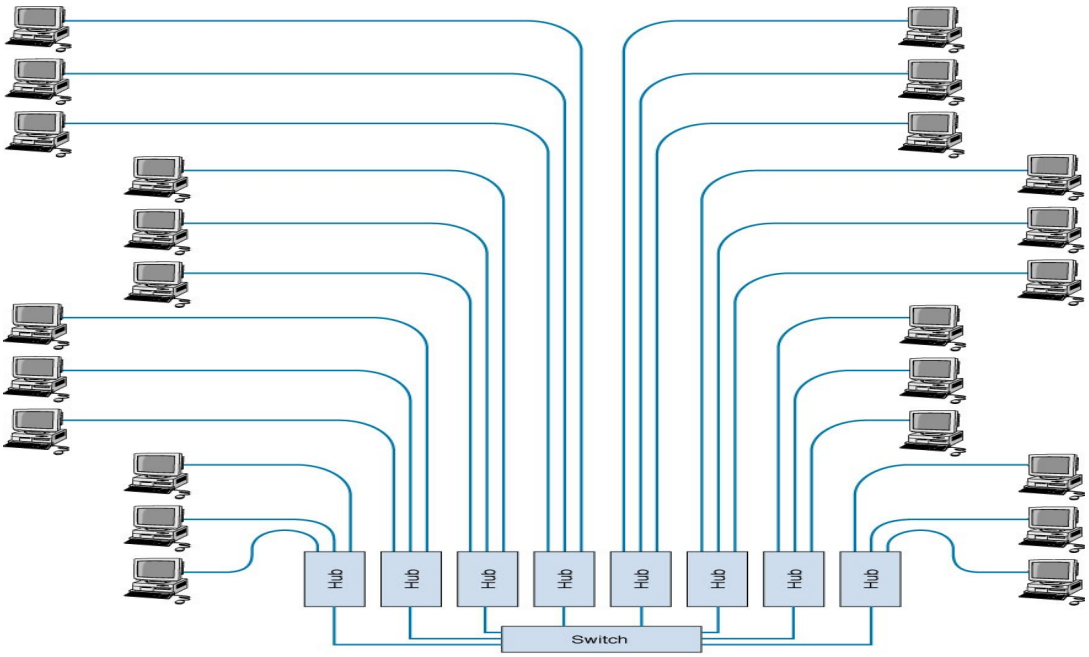
Collapsed Backbones

- Collapsed backbones use a star topology, usually with a switch at the center.
- This replaces the many routers or bridges of the previous designs, so the backbone has more cable, but fewer devices.
- Each connection to the switch becomes a separate point-to-point circuit.
- Advantages are: 1) simultaneous access and much higher performance (from 200-600% higher) and 2) a simpler more easily managed network.
- Two minor disadvantages are: 1) use more cable and the cable runs for longer distances, 2) if the central switch fails, the network goes down.



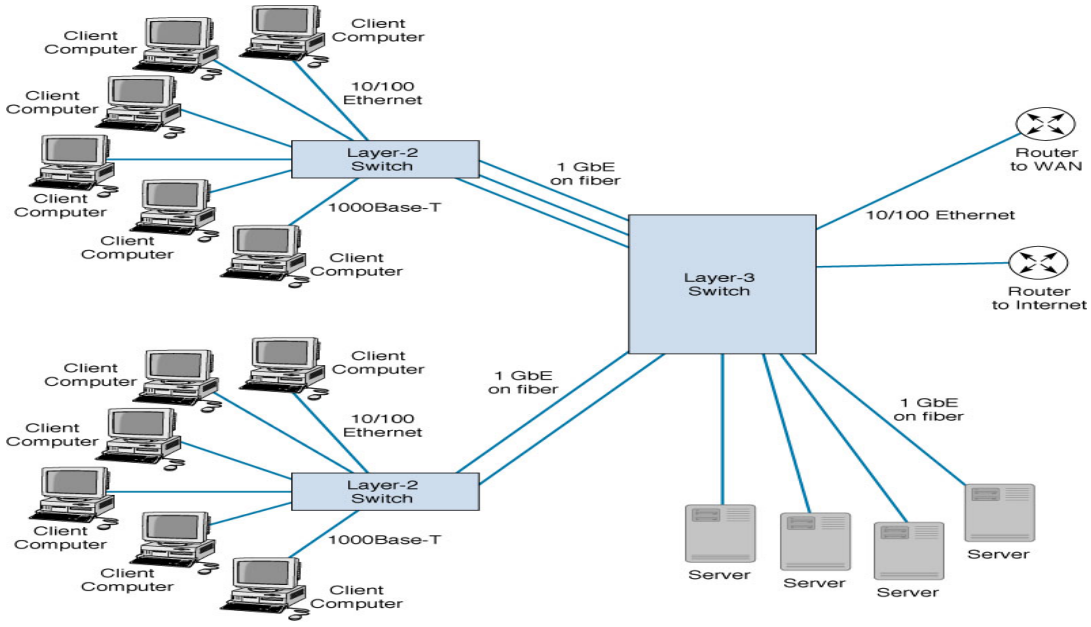
Rack-based Collapsed Backbones

- Rack-based backbones collapse the backbone into a single room, called a **main distribution facility (MDF)** where networking equipment is connected and mounted on equipment racks.
- Devices are connected using short **patch cables**.
- Moving computers between LANs is relatively simple since equipment is all in the same location.



Chassis-based Collapsed Backbones

- Uses a large chassis switch that has slots into which modules (i.e., card-mounted networking devices) can be inserted.
- Chassis switch designs include a number of open slots and have an internal capacity capable of supporting all active modules.

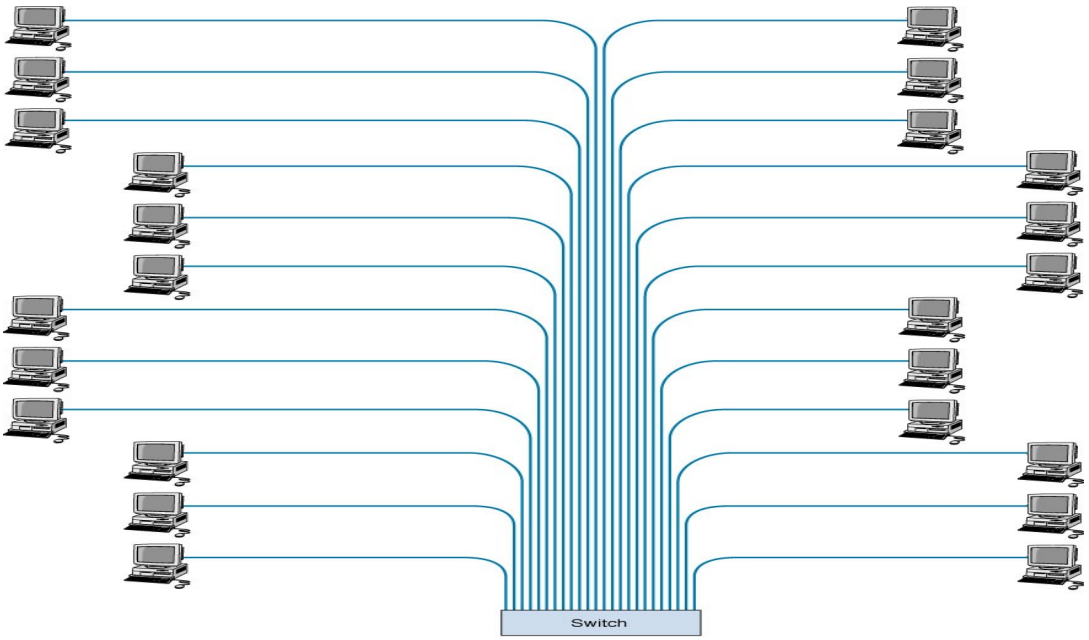


Virtual LANs

- VLAN is a new type of LAN/BN architecture that uses high-speed intelligent switches.
- In a VLAN, computers are assigned to LAN segments by software.
- VLANs are often faster and provide more flexible network management than traditional LAN and BN designs.
- They are also more complex and so far usually used for larger networks.
- The two basic designs are single switch and multi-switch VLANs.

Single Switch VLANs

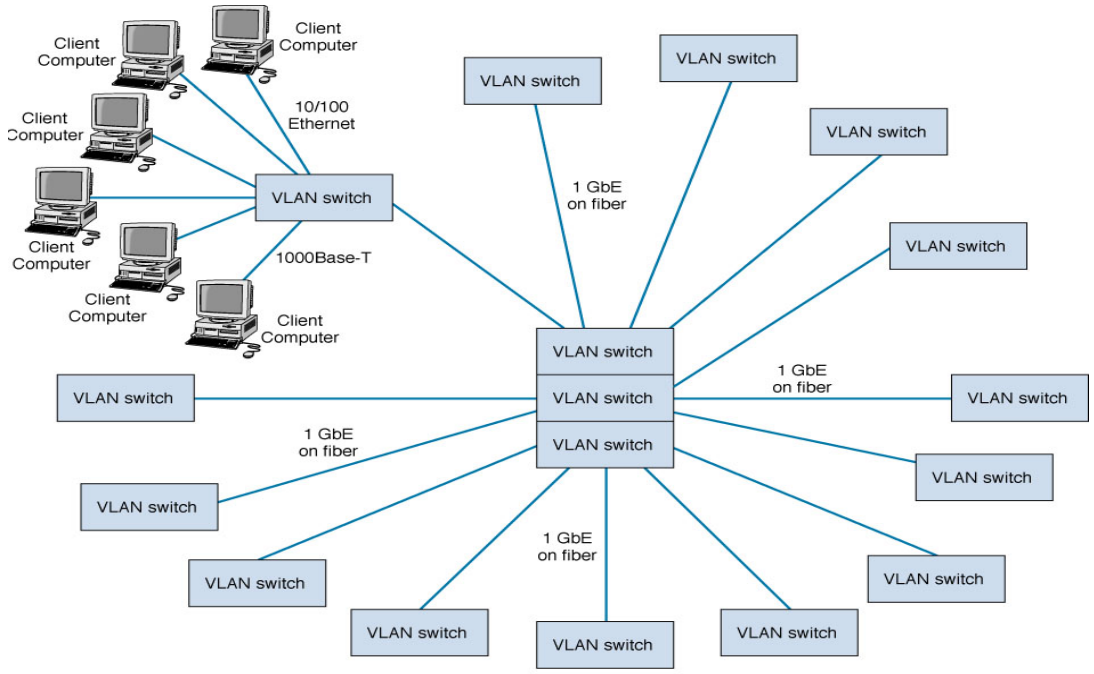
- This VLAN design connects computers using a single switch acting as a large physical switch.
- Computers are assigned to individual VLANs through software in one of four ways:
  - **Port-based VLANs** assign computers according to the VLAN switch port to which they are attached
  - **MAC-based VLANs** assign computers according each computer's data link layer address
  - **IP-based VLANs** assign computers using their IP-address
  - **Application-based VLANs** assign computers depending on the application that the computer typically uses. This has the advantage of allowing precise allocation of network capacity.



Multi-switch VLANs

- Multi-switch VLANs use multiple VLAN switches, sending packets among themselves, making new types of VLANs possible, such as VLANs in separate locations.
- Two approaches to implementing multi-switch VLANs are now in use. In one case proprietary protocols are used to envelope the Ethernet frame, which is then sent to its destination switch, where the Ethernet packet is released and sent to its destination computer.

The other approach is to modify the Ethernet packet to include VLAN information. The IEEE 802.1q standard adds 16 bytes of overhead onto the IEEE 802.3 Ethernet packet. When an Ethernet packet reaches a VLAN switch, it is set inside an IEEE 802.1q packet. When the IEEE 802.1q packet reaches its destination switch, its header is stripped off and the Ethernet packet inside is sent to its destination computer. [10]



1.8. Communication transmission means

There can be multitude of transmission media used for communication starting from copper wires, fibres and ending with radio and satellite means. Their deployment depends on the network size purpose and requirements. Over last years the communication links systems have been evolving to face the new challenges. As core networks are in focus, this section gives brief overview of the transmission means used in backbone environments.

1.8.1. T1 and T3

During last 20 years, T1 (1.5 Mbps) and T3 (45 Mbps) have ruled among solutions provided by carriers. T1 could provide 24 separate circuits, which brings benefits for multiple lines and sites communication management and cost efficiency. Besides, as T1 being digital communication system, they provided improvement versus analog lines in terms of higher resistance against noise and distortion. Analog amplifiers enhance the signal together with the noise, whereas regenerators used in digital communication can regenerate original signal without amplifying the noise. As commercial communication services developed, T3 appeared as next level in digital hierarchy. T3 link is made up of 28 T1s by means of dual step signal multiplexing.

1.8.2. SONET2

Eventually, evolution turned towards high-speed digital transmission resulting with SONET development. The synchronous bit streams in form of synchronous transport signals (STS), ranging from STS-1 (51.48 Mbps) to STS-48 (2.48832 Gbps) or higher, are scrambled, converted into optical form and transmitted through optical carriers (OC-1 to OC-48) and terminated by electronic switches. Such synchronous transport systems seemed to promise superior features for broadband communications.

1.8.3.ATM networks

Another turn in network evolution is related to emergence of broadband integrated services digital network (B-ISDN) supporting various multimedia services within a common network. Then, the ATM cell-switching technique seemed promising as transport means for a range of applications that require wide ranges of bandwidth together with quality of service. Typically ATM network configuration is based on a virtual topology consisting of dedicated virtual paths (VPs)

traversing via ATM switches. The VPs used to carry multiple virtual channels (VCs) that by match of corresponding characteristics can be suited to provide required quality of service for customer applications.

1.8.4. IP networks

With the Internet global scope flexibility, openness and scalability of IP, one of the earliest packet-switching protocols, let the IP protocol suite gain popularity and became a de facto standard in internetworking. The IP networks owe their recognition due to highly dynamic structure, where interconnected networks are free to change in topology structure and size. Well-regarded feature of IP network is its automatic topology recognition mechanism by means of IP routing protocols. [MON] [BN]

1.9. Economy of networking business

Among many other factors, the network development is driven also by the industry. Thus, it is worth to realize the commercial aspects as well.

The essential changes seen within telecommunication over last few years have been also implied by globalization and liberalization of the markets. In order to face the current desires network providers struggle to keep up with the market needs. The huge bandwidth promises associated with optical transport have brought more costs than revenues yet in fact. The recent collapse in economy also contributes to the fact that most corporations focus on saving opportunities together with maximum reduction of expenses.

Thus, backbone networks providers make great effort to offer attractive and profitable services for demanding access networks users and adhere to their SLAs. Furthermore, they have to deal with ominous economy implying priorities such as cost saving, efficiency in resource utilization, possible reuse of technologies and equipment.

1.10. Network requirements evolution

1.10.1 Internet development

Over last 20 years, the Internet became essential instance of every day life and powerful driving force for running business on

worldwide scope. The World Wide Web (WWW) has quickly gained popularity and expanded very rapidly. Also, more and more multimedia-oriented content has triggered escalating multicast and broadcast traffic. The Internet core has been constantly extended and upgraded to handle increasing in volume and quality demand end-to-end traffic.

Evidently, IP has emerged as 'de facto' standard for data communication and stimulus for global inter-working. However, its best-effort service turns out insufficient for the multitude of innovative and demanding applications that hit the today's market.

1.10.2 Side-effects

Calls for greater speeds and capacities

The broad and still spreading network ranges as well as exponentially increasing traffic volumes impose considerable requirements for scalability and high network capacities. In early 80's the T1 and T3 links connecting the routers in leased lines fashion were reasonable enough. However, the 90's brought new huge traffic volumes that could not be accommodated by the actual system. Soon the major carriers' speeds got increased to OC-3 (155 Mbps), OC- 12 (622 Mbps) and eventually to OC-45 (2.5 Gbp) and further up. Certainly, the upgrades involved not only the links but also Network Access Points (NAPs) and secondary proprietary backbones.

Internet environment

Main effect that is to be noticed in the Internet development is its unruly nature. There are multiple standards and coexisting technologies that compose an inter-working mixture. Apparently, providing management and reliability becomes serious trouble in such heterogeneous environment.

Another consequence raises importance of analysing reasonably technical, practical interoperation and economical aspects of approaching solutions that are to be implemented in such arena.

Routing scheme

Moreover, traditional routing scheme, based on shortest path choice, contributes to congestion problems. This way the great

deficiency of Interior Gateway Protocol (IGP) has been revealed, calling for some means that could enable more explicit and accountable traffic distribution and management in the network.

Router technology

Not long time ago, the router technology, with poor packet processing capabilities and moderate available interface cards, was underdeveloped to cope with the huge amounts of traffic. Thus, the software-based routing became a real bottleneck at that time. Also, management and processing of rapidly growing routing tables introduced troubles.

Earlier solutions

However, most common solution involved just purchasing more capacities. Simple over-dimensioning acting against the 'jams' is neither perspective nor economical. Still, the under-utilized spots make the capacity investment non-efficient. Efforts to manually distribute the load evenly throughout the resources with metric manipulation become difficult, not to say impossible, for large networks being more densely meshed with redundant connections. Besides, traffic characteristics or any dynamic changes of available resources are not accounted in this labour-intensive approach. When traffic flows demand are to be accounted, it should be noted that for drastically increasing traffic volumes with various delay-sensitivity, the capacity investment may appear a short term solution if the traffic quality guarantees are to be sustained. In reality, the old Internet core is incapable of providing quality for more demanding traffic streams, since the delays are unpredictable and very often exceed 150 or even 250 ms, which is unacceptable for voice communication.

1.10.3. Present networks requirements

All the mentioned development factors impose specific requirements on modern communication systems. They call for huge capacities, high reliability, enhanced performance and security. All these phenomena give good reasons for technical solutions and add to complexity and high significance of network planning, management and control. These necessities are foundation for such technologies as DWDM, SONET/SDH, ATM or MPLS.

However, the diversity of approaches does not make the network an easily manageable system. Multi-layered model seems luxurious

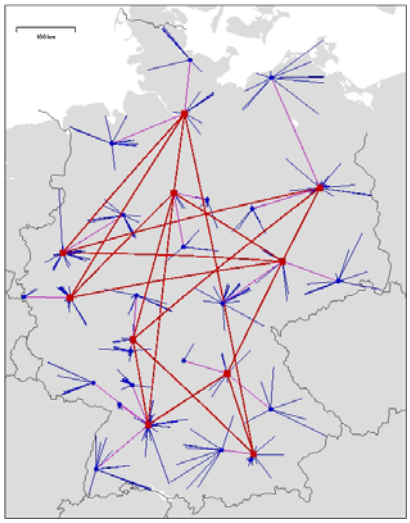
but in fact is very expensive and complex to handle in practice. The variety of existing networking standards together with proprietary aspirations from the industry contribute to the picture of diverse network we see at the moment. There have been appeals directing attention towards some point of uniformity. The concerns involve research on kind of common plane that would enable control over the whole heterogeneous multi-layer environment (e.g. GMPLS).[4]

2. Planning and Designing Principles

2.1. Planning Strategy

Considering the different solutions/network architectures that exist, each Network Planning case has to be analyzed and dealt with by using more than just one planning tool. It means that maintaining and updating a unique tool is not the correct strategy to be applied for Network Planning.[5]

2.2. Location Planning



The design of an appropriate structure for a large network is a complex task. In general, this planning problem can be described as follows: (i) for each location, decide which hierarchy level it belongs to, (ii) connect each location (except for the backbone) to the next higher hierarchy level, (iii) decide about the topology, the hardware configuration, and the capacities of the backbone network, and (iv) identify a routing of the communication demands which respects the installed capacities. The objective is to minimize the sum of connection and infrastructure cost.

There are different solution approaches. One of theme is a two-phase approach that splits the entire planning problem into two subproblems which are solved sequentially. In the first step, we only consider the structural design of the network hierarchy and the access network design. This subproblem can be viewed as capacitated multi-level facility location problem and is solved by integer linear programming techniques. Then, in the second phase, the backbone dimensioning and routing problem is addressed with the methods developed in work-package *Network Design and Routing*. The initial G-WiN design shown in the picture was computed with this two-phase approach.

A second integrated approach was developed in cooperation with Project Integrated Planning of Multi-level / Multi-layer Networks. This approach uses a combination of mixed-integer linear programming and Lagrangian relaxation techniques to solve the entire planning problem

without decomposing it into structural, access, and backbone network planning.[6]

2.3. Network Design and Routing

Designing a backbone network is hard. On one hand, user expect the network to have very high availability, little or no congestion, and hence little or no queueing delay. On the other hand, traffic conditions are always changing. Over time usage patterns evolve, customers come and go, new applications are deployed, and the traffic matrices of one year are quite different from the next. Yet the network operator must design for low congestion over the multiple years that the network is in operation. Harder still, the network must be designed to work well under a variety of link and route failures. It is not surprising that most networks today are enormously overprovisioned, with typical utilizations around 10%.

Network design can be formulated as an optimization problem where total cost is minimized subject to topology, demand, and performance constraints. The designer chooses where nodes and links are placed, their capacities, and how traffic is routed. On the face of it, this seems like a straightforward problem. We first determine the constraints on node and link location, and the expected demand, and then do our best to design an optimal network. In this paper, we will focus on designing a backbone network. Once deployed, the expense of the infrastructure dictates that the backbone topology (i.e., the set of nodes and their interconnectivity) doesn't change for several years. As traffic patterns change, and usage grows, a new topology will eventually need to be deployed, and the design process starts over. A well-designed network should support the traffic matrices presented to it for as long as possible. In the rest of this section, we will discuss some of the many challenges this presents to network designers today.[9]

In this work-package, we study the backbone network design and routing problem. In this problem, we have to decide simultaneously (i) the topology of the network, (ii) the link capacities, (iii) the installed hardware at the nodes, and (iv) a routing of the communication demands that respects the capacities.

Depending on the planning horizon different objectives are considered. For long and mid-term strategic planning, the task is to compute a cost-minimal design (or expansion) of the (existing) network while respecting certain QoS-constraints. In short term

planning, the goal is to adapt the traffic flows to the existing capacities by changing the routing only.[6]

A network and its backbone are based on the needs of the business, can be easily maintained, is fault tolerant, generally support lots of bandwidth for all current users (and future users), and have the ability to be expanded. Now that very last statement, has the ability to be expanded is fairly vague so let me clarify. Expansion ability should allow for more ports, as well as, new technologies. For example, if you have a core switch that utilizes blade technology and you would like to expand to 10GBE you should only have to purchase a 10GBE blade not a new core right.[3]

2.4. Failures and Routing Convergence

A network must be designed to continue to operate when there are failures and service or maintenance interruptions in the network. Failures cause two problems: Loss of connectivity, which can take several seconds to recover from [3], and is too slow for real-time applications such as voice and gaming. Second, failures demand extra capacity to carry rerouted traffic. Today, rerouting leads to large, coarse flows suddenly traversing a link, requiring large chunks of spare capacity. It is hard enough to design a predictable network when all links and routers are functioning correctly; it is even harder to ensure predictable behavior when there
are unpredictable failures.

2.5. Network Design in Practice

While network design can be formulated as an optimization problem, networks are not designed this way in practice. Juggling the number of constraints, estimates, and unknowns means that network design is more of an art than a science, and is dominated by a number of rules-of-thumb that have been learned over the years. This explains why each network operator has built a very different backbone network. Ad-hoc design makes it hard or impossible to predict how a network will perform over a wide variety of conditions. To offset the intrinsic inaccuracies in the design process, it is common to use traffic engineering in which operators monitor link utilization and route flows to reduce congestion, especially during failures.

Traffic engineering only works if the underlying network is able to support the current traffic matrix. With the complicated topologies

deployed today, it is not generally possible to determine the set of traffic matrices that a backbone network can support.[9]

2.6. Bandwidth Management

Bandwidth management is about making sure that enough bandwidth is available to meet traffic needs, and if not, managing the traffic in some way to ensure that critical traffic gets through. There are a number of topics that deal with bandwidth management. Refer to the following topics for more information:

- **QoS (Quality of Service)** This is the major topic that covers the many ways that users and services are provided enough network bandwidth to ensure that data is delivered with minimal delay and packet loss.
- **CoS (Class of Service)** CoS is a level of service that is promised to a client, not to be confused with QoS (quality of service). For example, you may choose next-day service from an express package service. That is a class of service. But the package may not arrive on time due to poor quality of service. You deserve a refund since the class of service you requested was not delivered.
- **Congestion Control Mechanisms** This topic discusses why networks, especially packet-switched networks, cannot always deliver COS or QoS, even when adequate bandwidth appears to be available.
- **Differentiated Services (Diff-Serv)** This topic covers work being done in the IETF Diff-Serv working group to define IP bandwidth management schemes using COS. In particular, the group is defining how to use the ToS (type of service) byte in the IP packet to identify prioritization of traffic.
- **Multimedia and Multimedia Networks** This topic is not about bandwidth management, but it talks about why you are going to need it.
- **Policy-Based Management** If bandwidth has to be allocated to specific users and applications in a fair (or unfair way), policies must be created to define who or what gets bandwidth and when. This topic describes how bandwidth is managed according to policies.
- **Traffic Management, Shaping, and Engineering** The best example of traffic management and "shaping" is to use the analogy of how traffic management is done on crowded freeways. At on ramps, traffic lights may admit cars every few

seconds in order to space them out and distribute the "load" on the freeway.

- **Load Balancing** With load balancing, redundant network links and/or network services are provided to spread loads across redundant links or systems. At a Web site, traffic may come in over multiple aggregate links to a load-balancing system that will hand packets off to the least busy server or a server that is most appropriate for processing the packet.

2.7. Quality of service

QoS (Quality of Service) determines a set of service requirements to be met by the network while transporting a connection or flow; the collective effect of service performance, which determine the degree of satisfaction of a user of the service. [E.360.1]

Within a backbone network, bandwidth expansion planning often begins with statistical estimation of network traffic. In addition to this information, we include the service level agreements with customers, wherein we assure them of a certain QoS (e.g. maximum latency or overall throughput etc.). Finally, we assume that the topology and the layout of existing capacity on the network.[8]

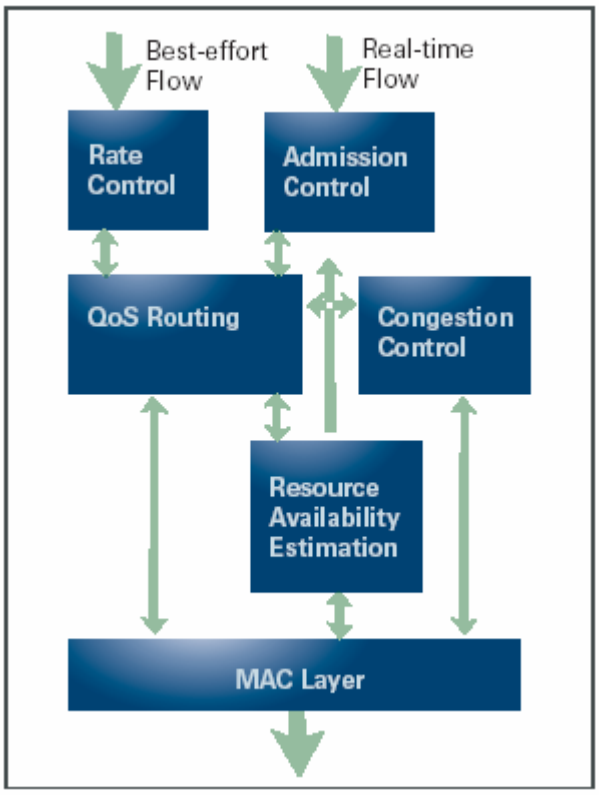
Situations that cause QoS to degrade are listed here:

- Shared network links, in which two or more users or devices must contend for the same communication channel.
- Delays caused by networking equipment (e.g., inability to process large loads).
- Delays caused by distance (satellite links) or excessive hops (cross-country or global routed networks).
- Network congestion, caused by overflowing queues and retransmission of dropped packets.
- Poorly managed network capacity or insufficient capacity. If a link has fixed bandwidth, the only option to improve performance is to manage QoS.

QoS Components

• Real-time Bandwidth Measurement
• Call Acceptance Control
• Soft Bandwidth Reservation

- Mobility Adaptation
- Scheduling with Policing
- Coexistence with Best Effort Traffic
- QoS Extensions of LANMAR, Fisheye, and AODV



Quality of Service Architecture. The model incorporated real-time bandwidth measurement and call acceptance control to manage QoS.

3. Traffic Engineering

As a consequence of requirements evolution, presented in previous section (1.10.Network requirements evolution), there are many challenges to overcome to increase performance and efficiency of modern networks. Main problems may be briefly pointed out as follows:

- Standard routing scheme does not account for resource utilization or routers performance characteristics,
- Load balancing is difficult to cope with in huge networks,
- Demanding traffic stream can hardly be guaranteed with any QoS,
- As all above points add up, in effect resiliency becomes particularly troublesome.

3.1. Network vs. traffic engineering

When considering the challenges mentioned above there are two crucial concepts that can bring remedy: network engineering and traffic engineering (TE). The first term concerns locating capacities concerned with long term planning, whereas the second idea deals with traffic organization in the network that is rather targeted for shorter periods. They can be associated with two indicated schemes: one focusing on development of high-capacity optical systems and the other directed towards logical traffic management. There could be two main observations noted: the network planning requires intervention within the network infrastructure, whereas TE appears demanding in terms of network management.

While network engineering is more manual and policy-dependent planning practice, TE is getting more directed towards automatic operation. TE concentrates within networking technologies and protocols, which targets current research society. The great interest towards TE originates also from the fact that the approach can provide facilities helping in overcoming many problems emerging in today's as well as next generation networks. Definitely, it may also bring higher return on network backbone infrastructure investment.

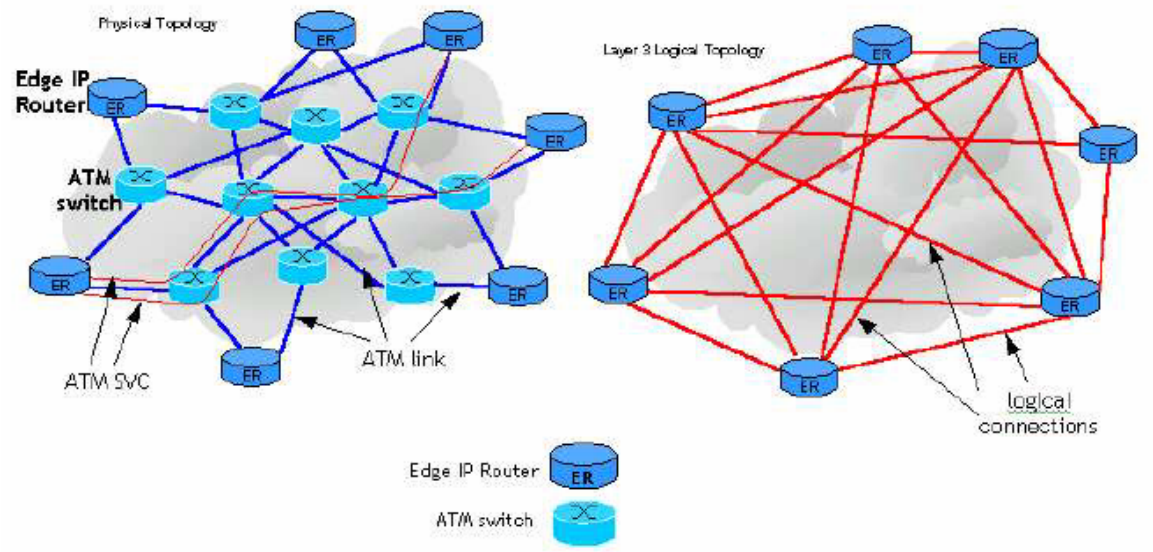
3.2. TE definition

It should be noted that TE is an abstract logical concept that should not be associated with specific implementation. The TE definition provides general idea without constraints for any particular practical employment. ITU-T defines TE in [E.360.1]: “Traffic engineering (TE) is an indispensable network function which controls a network's response to traffic demands and other stimuli, such as network failures.”

Furthermore TE is said to comprise traffic management, capacity management, traffic measurement and modelling, network modelling, and performance analysis. ITU-T defines also methods for TE. They involve network functions that support call routing, connection routing, QoS resource management, routing table management, and capacity management.

3.3. ATM (Asynchronous Transfer Mode)

ATM is a high-speed network technology that is designed for LANs, WANs, carrier and service provider networks, and Internet core networks. It is a connection-oriented switching technology, as opposed to a connectionless technology such as IP. ATM creates a virtual circuit (dedicated path) between source and destination across its switching fabric. These circuits can guarantee bandwidth and quality-of-service.



ATM overlay model

ATM's fixed cell size provides performance and predictable traffic flows. Picture a busy intersection. A semi tractor-trailer is attempting to negotiate a tight turn. All the rest of the traffic in the intersection is held up while this happens. Now picture the same intersection where all the vehicles are sports cars. In the latter case, traffic flows smoothly, and even predictably, because there are no traffic jams.

ATM cells negotiate ATM switches with the same efficiency, providing several benefits:

- Cell switching is efficient and fast for the reasons just described.
- Traffic flow is predictable due to the fixed cell size.
- Delivery of time-sensitive traffic (live voice and video) can be guaranteed.
- ATM includes QoS (quality of service) features that can be used to guarantee bandwidth for certain types of traffic.

There has been great debate over whether ATM is better than IP and vice versa. Many people find this debate odd, since the technologies are quite different and not even in the same protocol layer. **The battle is really about whether networks should be *connection oriented* (ATM) or *best effort* (IP).** ATM's fixed cell size and virtual circuit capability makes it the best choice for real time multimedia. Carriers and service providers use ATM in their core networks because it lets them provide service guarantees to their customers. However, IP's simple packet forwarding model has proved its usefulness in the Internet, where traffic is bursty and unpredictable. This model allows millions of people to share the bandwidth of the Internet without setting up virtual circuits in advance. However, the IP model starts to break down under traffic loads and congestion. In addition, the unpredictable delays of IP networks are a problem for real-time traffic.

ATM was originally defined by the telephone companies and has been heavily promoted by them as an end-to-end networking technology, as well as a voice technology. In this respect, ATM is both a LAN and WAN technology that can potentially allow customers to replace their separate voice and data networks with a single network to handle both voice and data, as well as other multimedia content such as video.

In the early 1990s, ATM was widely considered the next-generation networking technology that would extend all the way to the desktop. But broadcast LANs were already entrenched in most

organizations and Internet technologies exploded on the scene. And while ATM was hyped for its speed, Gigabit Ethernet (1,000 Mbits/sec) and now 10 Gigabit Ethernet offer cheaper and more easily managed services.

Still, ATM is a viable technology for backbones, even in Gigabit Ethernet environments. ATM is easily scalable and integrates with most existing technologies.

More recently, new technologies such as DWDM (Dense Wave-Division Multiplexing) and optical networking may undo ATM and even SONET. DWDM puts hundreds and potentially thousands of lambda circuits on a single fiber. That means core networks will support very high capacity switched optical circuits, reducing the need for packet switched core networks. Imagine having an entire beam (wavelength) of light allocated for your personal use, switched into place when you need it and taken down when you have finished. That is what the new optical networks could provide.

3.4. Gigabit Ethernet

Gigabit Ethernet is a 1-gigabit/sec (1,000-Mbit/sec) extension of the IEEE 802.3 Ethernet networking standard. Its primary niches are corporate LANs, campus networks, and service provider networks where it can be used to tie together existing 10-Mbit/sec and 100-Mbit/sec Ethernet networks. Gigabit Ethernet can replace 100-Mbit/sec FDDI (Fiber Distributed Data Interface) and Fast Ethernet backbones, and it competes with ATM (Asynchronous Transfer Mode) as a core networking technology. Many ISPs use Gigabit Ethernet in their data centers.

Gigabit Ethernet provides an ideal upgrade path for existing Ethernet-based networks. It can be installed as a backbone network while retaining the existing investment in Ethernet hubs, switches, and wiring plants. In addition, management tools can be retained, although network analyzers will require updates to handle the higher speed.

Gigabit Ethernet provides an alternative to ATM as a high-speed networking technology. While ATM has built-in QoS (quality of service) to support real-time network traffic, Gigabit Ethernet may be able to provide a high level of service quality by providing more bandwidth than is needed.

3.5. 10-Gigabit Ethernet

As if 1 Gbits/sec wasn't enough, the IEEE is working to define 10-Gigabit Ethernet (sometimes called "10 GE"). The new standard is being developed by the IEEE 802.3ae Working Group. Service providers will be the first to take advantage of this standard. It is being deployed in emerging metro-Ethernet networks.

As with 1-Gigabit Ethernet, 10-Gigabit Ethernet will preserve the 802.3 Ethernet frame format, as well as minimum and maximum frame sizes. It will support full-duplex operation only. The topology is star-wired LANs that use point-to-point links, and structured cabling topologies. 802.3ad link aggregation will also be supported.

The new standard will support new multimedia applications, distributed processing, imaging, medical, CAD/CAM, and a variety of other applications-many that cannot even be perceived today. Most certainly it will be used in service provider data centers and as part of metropolitan area networks. The technology will also be useful in the SAN (Storage Area Network) environment. Refer to the following Web sites for more information.

3.6. MPLS (Multiprotocol Label Switching)

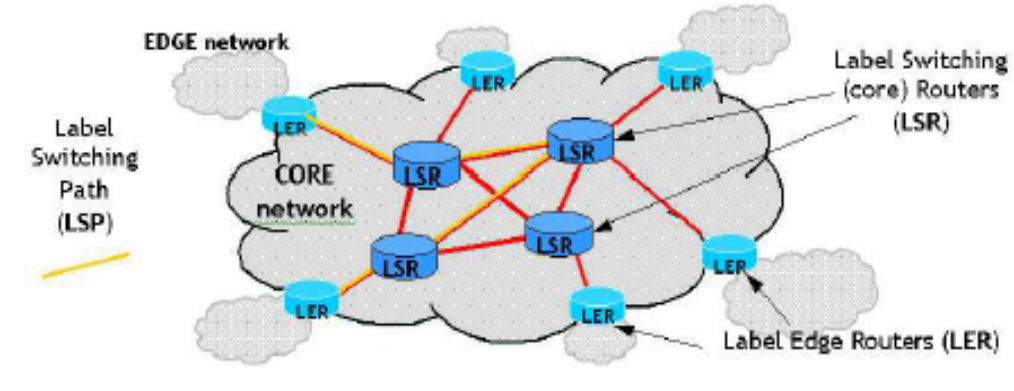
MPLS is an IETF-defined protocol that overcomes some of the shortcomings of IP-based networks. MPLS is meant for service provider core networks or large enterprise networks. It brings traffic engineering, bandwidth management, and quality of service to IP networks. A form of MPLS is used to set up and manage wavelength optical circuits (lambdas) on the core optical networks of the Internet.

MPLS's key feature is the ability to build virtual circuits across IP networks. These VCs are called label switched paths (LSPs). LSPs are similar to virtual circuits in ATM and frame relay networks. Labels are attached to packets, which help MPLS nodes forward the packet across an LSP. The labels are like tracking slips on express delivery packages. They contain an index into a forwarding table, which specifies the next hop for the packet. Nodes in the core MPLS network do not need to examine packets and perform next-hop routing tasks. The label carries the information that determines which path a packet should take.

MPLS supports traffic engineering to provide traffic prioritization and QoS. For example, a path can be created that provides high bandwidth and low delay for "premium" customers who are willing to pay for it. In another example, multiple paths can be defined between two endpoints to provide load balancing and backup service in the event of a line failure. This is similar to using metrics in IP routing to force traffic in one direction or another, but it is much more powerful.

Paths can be engineered using manual or automatic techniques. MPLS supports explicit routing, in which network engineers define specific paths across a network for specific types of traffic. MPLS also supports constraint-based routing, in which the path is selected on-the-fly as a packet traverses the network, based on parameters that constrain the forwarding direction. Constraint-based routing involves programming traffic-engineering parameters into the network.

An MPLS network is typically a large group of core switches that span a large geographic area, usually an entire country. AT&T, Global Crossing, and other providers have MPLS networks. MPLS may also be used in metropolitan area networks. Terabeam uses MPLS in its "Fiberless Optical" network. Periphery networks are attached to the edges of the MPLS network via LERs (label edge routers), as shown in Figure. The core contains LSRs (label switching routers). The periphery networks may be operated by regional ISPs, local network operators, or even private companies.



MPLS network infrastructure

MPLS is an IETF specification based on label switching approaches developed by several vendors, including Cisco (Tag Switching), IBM (ARIS or Aggregate Route-Based IP Switching), and

Lucent/Ascend (IP Navigator, originally developed by Cascade). MPLS integrates layer 2 switching and layer 3 routing. For ATM switches, MPLS adds routing functionality, creating a hybrid switching router. Layer 3 components are IP routing controls (OSPF and BGP), which replaces standard ATM Forum routing and control protocols.

Prior to these approaches, several techniques were developed to overlay IP on top of ATM. The ATM Forum's MPOA (Multiprotocol over ATM) is an example. The overlay models provide shortcut routing of IP packets across an ATM backbone, but the underlying ATM network protocols are used unchanged. However, these earlier techniques were not as scalable as MPLS.

MPLS Basic Operation

As shown in Figure, LSRs are core devices that switch packets, and LERs are edge devices that connect with external networks, determine routes, and add or remove labels. An LSP is a concatenation of switch hops that form an end-to-end forwarding path. An LSP starts at an ingress LER, crosses one or more LSRs, and ends at an egress LER.

When a packet arrives at an MPLS network, the ingress LER does most of the work of handling the packet. It looks at the packet's IP address, determines a route, assigns an LSP, and attaches a label. The packet is then forwarded into the LSP, where it is switched across a series of LSRs until it reaches the egress LER. The label is removed and the packet is forwarded on its way via standard IP routing.

3.7. Optical Networks

An optical network is a network in which the physical layer technology is fiber-optic cable. Cable trunks are interconnected with optical cross-connects (OXCs), and signals are added and dropped at optical add/drop multiplexers (OADMs). The holy grail is an all-optical network. In this scheme, an optical wavelength (which acts like a data circuit) stays in the optical realm from end to end.

In contrast, most optical networks have implemented OEO (optical-electrical-optical) switches, which convert optical signals to electrical signals for processing, and then back again to optical signals for the next leg of the trip. The optical-to-electrical conversion adds delay and introduces possible errors as the signals are converted,

moved up the protocol stack, and processed by software or firmware. The all-optical network avoids this process. At this writing, components that make the all-optical network a reality are emerging.

3.7. SONET (Synchronous Optical Network)

SONET is a standard that defines telecommunication transmissions over fiber-optic cables. It defines the access methods, framing, and other parameters for transporting digital information over an optical communication system. SONET was first proposed by Bellcore (now Telcordia) in the mid-1980s, and then standardized by the ANSI (American National Standards Institute). The ITU adapted SONET to create SDH (Synchronous Digital Hierarchy), a worldwide telecommunication standard. SONET is a subset of SDH that is used in North America. SONET technology issues are managed by NSIF (Network and Services Integration Forum).

SONET was designed as a means to deploy a global telecommunication system, and so SONET/SDH is widely deployed by the world carriers. It uses standardized rates to ensure that telecommunication companies around the globe can interconnect their systems with little trouble. SONET removes the boundaries between the telephone companies of the world. But SONET is not limited to carrier networks. SONET may run directly to large enterprises in metropolitan areas or be used to build campus networks.

WDM (Wavelength Division Multiplexing)

WDM is an FDM (frequency division multiplexing) technique for fiber-optic cable in which multiple optical signal channels are carried across a single strand of fiber at different wavelengths of light. These channels are also called lambda circuits. Think of each wavelength as a different color of light in the infrared range that can carry data.

A fiber-optic cable guides light from end to end. A signal is injected in one end by an LED (light-emitting diode) or by

semiconductor lasers. Lasers for silica-based fiber-optic cables produce light in a range called a "window." These windows occupy the near infrared range at wavelengths of 850 nm (nanometer or billionths of a meter), 1,320 nm, 1,400 nm, 1,550 nm, and 1,620 nm. For example, you may see a system described as a 1,550-nm system. Optical multiplexers divide the window into many individual lambdas. Figure W-1 illustrates the output of a 16-channel WDM system operating in the 1,530- to 1,565-nm range. Each lambda circuit is capable of transmitting 2.5 Gbits/sec for a total of 40 Gbits/sec.

As mentioned, optical systems are discussed in terms of their wavelengths (in nanometers). For comparison, red blood corpuscles are about the same size as the wavelengths in the infrared range. A wavelength of 1,550 nm has a frequency of 194,000 GHz (194,000 billion cycles/sec). The frequency increases as the wavelength is shortened. A decrease of only 1 nm increases the frequency by 133 GHz. This is used to advantage by Avanex in its PowerMux optical multiplexer. The PowerMux can put over 800 channels on a single fiber. It separates channels by 12.5 GHz or 0.1 nm. The Avanex Web site (http://www.avanex.com) provides some interesting information about optical systems.

WDM is employed by carriers such as MCI to boost the data rates of their networks dramatically. MCI incorporated Quad WDM (four-wavelength WDM) in its backbone several years ago, instantly quadrupling its network capacity. The backbone operated at 2.5 Gbits/sec before Quad-WDM and at 10 Gbits/sec after installing Quad-WDM multiplexer devices. Since then, MCI has been upgrading to higher-capacity systems.

There are three categories of wavelength division multiplexing:

- WDM (wavelength division multiplexing) Two to four wavelengths per fiber. The original WDM systems were dual-channel 1310/1550 nm systems.
- CWDM (coarse wavelength division multiplexing) From four to 8 wavelengths per fiber, sometimes more. Designed for short to medium-haul networks (regional and metropolitan area).

- DWDM (dense wavelength division multiplexing) A typical DWDM system supports eight or more wavelengths. Emerging systems support hundreds of wavelengths.

The spacing between wavelengths in CWDM is about 10 to 20 nm, while the spacing in DWDM is about 1 to 2 nm. Due to the tight spacing and number of lasers, DWDM systems require elaborate cooling systems. Also, precision light sources and complex optical multiplexers are required to ensure that channels do not interfere with one another. In contrast, CWDM systems are simple and easy to manufacture, and cost much less than DWDM systems. They are also smaller. A CWDM device can be held in your hand, while a DWDM device is a large box that requires rack mounting.

The development of EDFAs (erbium-doped fiber amplifiers) provided a boost in cable distance and capacity for fiber-optic networks. EDFAs can amplify optical signals directly by injecting light into the cable via a light pump. Weak signals enter the amplifier and stimulate excited erbium atoms in the erbium-doped fiber to emit more light, thus preserving the original signal and boosting its output signal. Best of all, EDFAs can simultaneously boost the signals of multiple wavelengths in the same cable. EDFAs work in the 1,500- to 1,600-nm range, so a typical DWDM system has a range of lambda circuits operating in this range.

Prior to the development of EDFAs, optoelectronic amplifiers were used to boost optical signals. The process is often called "3R" regeneration, referring to reamplify, regenerate, and retime. Weak incoming light is converted to a voltage signal, amplified, and then converted back to light. This is impractical in high-speed core networks.

With the potential of hundreds of lambdas per fiber, it is practical for carriers to lease entire optical circuits to businesses. For example, a television network could lease lambda circuits to transmit video signals among media centers and stations. Recently, MPLS

(Multiprotocol Label Switching) has been considered an ideal protocol for controlling optical switches in DWDM networks. It already controls LSPs (label switched paths) across routed networks and can also be used to control optical paths.

Basic traffic trunk attributes related to TE are summarized in Table 3.1 below. Most of them can find their analogies in other technologies like ATM.

Table 3.1.Traffic trunk attributes for TE

traffic trunk ATTRIBUTES for TE	DESCRIPTION
traffic parameters	reflect traffic characteristics that can be used for FEC carried within traffic trunk; they may include e.g. peak rates, average rates, permissible burst size, etc.
generic path selection and management	identify principles for route selection for traffic trunk as well as rules for maintenance of already established paths
priority	binary relation determining the manner in which traffic trunks interact with each other while they compete for network resources during path maintenance
preemption	binary relation determining the manner in which traffic trunks interact with each other while they compete for network resources during path establishment
resilience	control behavior of the trunk under fault situations
policing	enable enforcing trunk compliance with SLAs

Appendix

Internet, Articles, Books

[1] www.pcmag.com/
PC Magazine - Computer, Software, Hardware and Electronics Reviews. Complete guide to PCs, peripherals and upgrades. Labs-based reviews of computer- and Internet-related products and services, technology news and trends.

[2] www.linktionary.com/ Tom Sheldon, 2003, 3rd edition
The Encyclopedia of Networking and Telecommunications

[3] http://networking.ittoolbox.com/blogs/featuredentry.asp?i=4295
Article: "A Challenge - Network and Network Backbone" by ThunderMace2000 (Network Administrator)

[4] Article Emilia Dabranowska

[5] ITU

[6]www.zib.de/Optimization/Projects/Telecom/G-WiN/G-WiNlong.en.html
ZIB: Optimization of the German Research Network G-WiN and Lagrangian relaxation techniques to solve the entire planning problem without decomposing it into structural, access, and backbone network planning.

[7] QualNet by Scalable Network Technologies, Los Angeles

[8] Suvarjeet Sen and Prasad Boddupalli, Raptor Lab, SIE department, University of Arizona, Tucson, AZ 85721

[9] Rui ZhangShen, Nick McKeown, Computer Systems Laboratory, Stanford University

[10] http://conta.uom.gr/

[11] http://www.eett.gr/

[12] http://www.gr-net.gr/

[13] http://www.iec.org/

[14] http://www.heal-link.gr/

[15] http://www.cisco.com/en/US/netsol/index.html

[16] http://www.knowledgestorm.com/

[17] Computer Networks, Andrew S. Tanenbaum, 3rd Edition