# Table of Contents

Network Design Concepts and Principles ......................................................... 1
  Executive Summary ............................................................................................. 1
  Background .......................................................................................................... 1
    Methodology ....................................................................................................... 1
  Network Design Concepts .................................................................................... 1
    Conceptual Simplicity ......................................................................................... 1
    Appropriate Sized Pipes ................................................................................... 1
    Flexibility ........................................................................................................... 1
    Holistic Security ................................................................................................. 1
    Continual Improvement ....................................................................................... 1
  Test ....................................................................................................................... 1
  Documentation ...................................................................................................... 1
Network Design Principles ..................................................................................... 1
  The Network Core ............................................................................................... 1
  Wireline and Wireless .......................................................................................... 1
  Data Facilities ...................................................................................................... 1
  Appropriate Security ............................................................................................ 1
Next Steps ............................................................................................................... 1
Appendix A - VLAN Considerations ................................................................. 1
Network Design Concepts and Principles

Executive Summary

Our consulting group was awarded the privilege of facilitating the University of New Mexico to produce the principles that will shape the next-generation network design. We began by first listening and understanding the requirements of the people who will be the users of the network. We conducted a series of initial interviews and a three-day facilitation exercise in order to understand these requirements. The interaction with these users inform the basis for our recommendations, which are articulated below.

The recommendations can be viewed as being two tiers - Concepts and Principles. Another, perhaps more useful, view is of a two dimensional matrix where concepts are on one axis and principles are on the other. Viewing the matrix shows how a concept applies to each principle and how a principle contains each concept. Together, they form the bedrock of what principles should be employed in a network core and the concepts each principle should embody.

The network of tomorrow will be defined by at least two important characteristics. It will be mobile and it will be porous. The University network encompasses a wide scope of specialties and capabilities. These concepts and principles will provide the appropriate level of robustness and controls to ensure the safety, requirements and needs of all segments of the University network and for those who interact with it.

Background

Methodology

The University of New Mexico IT organization requested assistance in facilitating the design of a next generation campus-plus network. We understood that to facilitate what the University wanted, we needed to first understand what all users, throughout the University of New Mexico, wanted and their associated requirements.

The University of New Mexico is composed of twelve colleges, branch campuses, and other tele-connected facilities. The network encompasses the University as well as research sites, hospitals, and a variety of remote and statewide facilities. The concepts and principles developed needed to address all segments of the University network, in order to form the bedrock of a network for the future. So we assembled users, customers and partners from all segments, into groups which we labeled Communities of Interest (COIs). COIs included Researchers throughout the University, the Research Park, Health Sciences, Telemedicine, etc. Students represented their own COI. Administration staff across all segments formed another as did Education composed of providers, staff, faculty, distance and online, etc. The Health Sciences Center included representation from the hospitals, the various medical schools, clinics, centers, physicians, etc. Lastly, a COI of those external bodies that currently have network needs included other higher education entities, K through twelve, government and partners.
COIs were designed to not closely correlate to any departments, divisions, or other existing
groups. The purpose was to minimize group think, repetitive input, and most importantly to be
disruptive. This structure helped us gain insight more easily than any other grouping could have.

Consequently, we embarked on a series of discussions with the communities themselves. In the
first phase, we conducted interviews with staff (and faculty, etc.) from all parts of the University
only. External groups such as other higher education entities, K through twelve, government and
partners were not included because they are not part of the University’s network, they are users.

In the second phase we held a series of facilitation meetings with a diverse set of community
members from each COI, so we could hear various interests' responses to the following high-
level questions:

- What interaction do you currently have with the various IT groups?
- What new or different interactions do you expect to have with these groups going
  forward?
- In what ways does the current network not meet your needs, expectations, or desires?
- In what ways do you expect your future network needs to change?

We would follow up these questions seeking additional depth. Sometimes our queries were
hypothetical, sometimes confrontational, sometimes general, sometimes detailed, and often we
just sat back and listened to what people had to say. We'd like to thank the UNM IT staff for
putting together what we feel was an excellent profile of University customers and partners for
these discussions. We'd also like to thank the participants who were extremely generous with
their time, and provided us with a great deal of insight into their respective information needs.

**Network Design Concepts**

Let’s get right to the purpose of this document. For this project, we believe that there are several
core ideas that should inform all of our architectural choices for a University-wide network of
the future. This section introduces these core ideas as network design concepts. Think of these
as the voices you should listen to when employing the Network Design Principles covered in the
next section.

We adhere to none of these philosophical concepts dogmatically. There are situations in which
we acknowledge that the right solution violates one or more of our cherished concepts.
However, when two solutions are possible, it is unlikely that we'd ever regret selecting the
solution that most closely adheres to these concepts.

**Conceptual Simplicity**

We take the common paraphrase of Albert Einstein to heart in network design and
implementation, "Everything should be made as simple as possible, but no simpler.” We seek to
minimize the complexity of a deployed system at every opportunity that does not compromise its
function. Doing so leads to flexibility in implementation and robustness in maintenance.
Maintaining a network with unnecessary dependencies, impedes the ability to repair or upgrade
that network which is exactly why we list this maxim first.
It would be simpler to not implement redundant connectivity to the outside world or at the
network core, but doing so compromises redundancy to an unacceptable level, so we live with
that amount of additional complexity. On the other hand, when adding extra links to a redundant
core, it is critical to ask, "What does this extra connection provide for us?" and "Is there a
simpler design that accomplishes the same goal?" If there is an affirmative answer to the second
question, we will inevitably prefer to implement that solution.

Sometimes time or financial constraints pressure us to implement a complex but inexpensive or
rapid solution. First, this urge should be resisted whenever possible. Inevitably, there will be
situations in which such a solution is pushed upon us by necessity. It’s not that such a fix should
never be implemented. Our principle of Conceptual Simplicity dictates that such a patch be
applied only on a short term basis. A job is never done until its done right.

An example of a violation of conceptual simplicity is if connectivity between two nodes ever
passes through the same device more than once. Another example is a failure to distinguish
between a redundant connection to a critical edge node and a part of the mesh core network.
Sometimes these may be the same thing, sometimes they're not. Any network design that doesn't
distinguish the two is likely to be inappropriately complex.

**Appropriate Sized Pipes**

Determining the appropriate size for bandwidth will almost always be tied to the service that is
being provided, the connections between the service and user and a myriad of external
influences. When we say *appropriate*, we're recognizing that just because a pipe of size x is big
and fast, it does not logically follow that a 2x pipe is a) two times faster than x, b) possible, or c)
appropriate. Another way to say this is that the appropriate size of a pipe cannot be considered
in a void. Everything about the external influences and connections enters into the determination
of what is appropriate.

We like that when you size pipes appropriately, they have a property that falls neatly into another
concept we've already mentioned in this section, they're *Conceptually Simple*. Further, this
simplicity makes them robust, and their use in nearly any context makes them *Flexible*.

So in an environment where Quality of Service (QoS) guarantees are necessary, one must
consider if the inappropriate size of the pipe (amount of bandwidth available) is the cause for
wanting QoS, or if it is being used for prioritization. Good design can certainly include the use
of QoS protocols and bandwidth reservation, especially as a protection against bursty loads. But,
good design never uses complex protocols by themselves, as a *fix* for network issues.

**Flexibility**

Information services are always in flux. New services are rolled out, organizations move from
one location to another, new facilities come on line, and even, on rare occasion, old services are
retired. Infrastructure should be built with the idea that it is straightforward to repurpose for
some other task, so we can save ourselves both time and money down the line. The previously
mentioned *Appropriate Sized Pipes* are an example of flexible design.
Holistic Security

IT security should not be an afterthought for a system or service. Holistic security means thinking of security by design; from the beginning and its affect on the whole. Before a system is rolled out or upgraded, it is important to not only consider the security aspects of the service, but how it will fit in to the overall organizational security schema. Moreover, a service rollout that requires a new security mechanism or adds complexity to the lives of its user community should be reevaluated for its compliance with the previously mentioned Conceptual Simplicity.

Use cases should be drawn up to illustrate how the new service will be used, and by whom. With those in hand, access rules are straightforward and should be deployed with the service. Whether users are internal, across departments or include external groups, limited access can be easily achieved in a holistic solution.

Continual Improvement

It is important to never become complacent about the quality of service provided. There is an enormous difference between thinking, "Aspect X of our service is running well enough now that it's not my top priority," and "Aspect X is running so well now that I don't need to think about it." It requires a special level of discipline to not lose sight of this, but we believe that this is one of the qualities that distinguishes the truly exceptional organizations.

Test

After developing any plan, be it development, replacement, migration, upgrade or any other plan that has an impact on the network, the actions should take place in a test environment, a test bed. This ensures that our assumptions and calculations are accurate. The only way to determine that the products and services used in the upgraded network will function as expected, is to perform as much extensive testing as is feasible.

Documentation

Just about everything should be documented, whether it is a network architecture diagram (from both a physical and logical perspective), to repeated procedures, to troubleshooting methods, to meeting minutes.

Documentation becomes a key part of an internal training regimen. People forget, or they move on to another responsibility. It is important that documentation include an executive overview that can be presented to upper management.

Documentation that reflects the ongoing operation should be reviewed and updated periodically. Not only does this mean that the documents need to reflect the organization and its services as they exist, in a manner that's usefully descriptive, but they also need to be cataloged and available in such a manner that those who are interested will be able to find them.
Network Design Principles

We’ve outlined above the seven concepts that are important considerations in the practice of network design; conceptual simplicity, appropriate sized pipes, flexibility, holistic security, continual improvement, testing and documentation.

In this section, we discuss the design principles for a University-wide next generation core network and how the relevancy of the aforementioned concepts influence them.

The Network Core

Redundancy and Structure

Having a core network with diverse pathways is a key ingredient of any truly robust campus-wide network (remote campuses and other like networks included). Not that this should mean there are multiple network connections between core nodes, but that these links are as physically diverse as possible. Multiple cables running in separate conduit from different buildings should be part of the core design whenever possible. One should also connect to all critical upstream nodes as well as high priority end nodes through diverse pathways as well.

Nearly every network of this scope should incorporate a fully redundant partial mesh architecture connecting the core and high-value end nodes, with star branches connecting the lower priority or prohibitively expensive end points. We’re not aware of any good reason to deviate from this architecture.

First, consider the level of network redundancy. Every core node and critical edge node should be connected to at least two (other) core nodes, but no more than necessary to fulfill its core and edge functionality. A full mesh is more expensive to deploy than a partial mesh, and while it provides some protection against some multiple failure modes, it also frequently increases overall complexity and convergence time in the event of a failure. Adding additional redundant links beyond those that will account for practical failure scenarios costs extra and frequently reduces rather than enhances robustness.

A switched core is more flexible than a routed core and generally offers more throughput at a lower price point - at the cost of some convergence time in case of an outage. Either architectural decision is legitimate.

We’re clearly setting the design principle preference of a mesh network for its many benefits, not the least of which is redundancy. Recognizing that cost is always a factor, you can connect low priority and/or prohibitively expensive end points with a star branch. This certainly isn’t the only network topology that is common or popular. Our analysis of requirements and needs, not dogmatic belief, lead to this principle.

Segmentation

The extensive use of VLAN technology is often a convenient way to solve networking problems. Inappropriate use of this technology leads to serious maintenance problems. Therefore, restraint
should be used when it comes to this technology. The reasons why, are more technical and advanced than the rest of this document, so we have moved them to Appendix A.

Generally, networks with users and services on them should be connected to the campus backbone by router ports. Connections between networks with different security levels or between organizations with autonomous IT groups should be separated and perhaps filtered as well.

Changing traffic patterns or new connections may require new dynamic circuits or linked using appropriate modern technology. Constant network tasks and services that are experiencing growth may make it desirable to increase network bandwidth by upgrading link capacity. It is always a good idea to map out the proper topology and then incrementally add and subtract links to achieve the new goal rather than just to add bandwidth or more cabling to the existing plant.

Wireline and Wireless

Despite the explosive growth and unqualified success of wireless networking over the last decade, the wireless Internet is not a replacement for wireline connections.

There are substantial reasons for the selection of wireline over wireless, but they are especially evident when there are high bandwidth networking requirements or special security considerations. The current state of wireless technology is such that it has limitations. Use should consider current capabilities.

Wireless Expansion

There are some tasks for which wireless connectivity is simply inadequate. At the same time, the explosive growth of wireless usage, demonstrates how it has become an indispensable service. Wireless deployments should continue with an emphasis on making more bandwidth and IP address space available to accommodate what currently appears to be a limitless expansion.

Wireless use has grown rapidly, in large part because of the pervasive nearly-always-on devices that aggressively grab available IP addresses, such as tablet computers and smart phones. Some education of the user community may help a little; teaching people to configure their devices to be less assertive in grabbing Wi-Fi IP addresses couldn't hurt. Unfortunately, the impact is like trying to stop the rising tide with a bucket.

Wireless upgrade plans need to be agile. This will mean evaluating and upgrading a flexible underlying network far more frequently than for wireline networks. Available tools should be used in order to frequently upgrade wireless capabilities to meet the seemingly ceaseless growth. Upgrade and new deployment of these services should be given as much latitude as possible to build out at an accelerated pace.

Build Out

It is tempting to think that some new buildings can be built without a cabling infrastructure. This is not recommended. Similarly, depending on a wireless infrastructure in a building that will or might some day support a user community with significant security or bandwidth needs all but
guarantees that eventually an expensive and inelegant retrofit will be required. This violates our flexibility guideline.

For any new building or renovation, IT should be involved early. The building customer will have information needs, and someone should speak to port distribution as well as how the building will be connected to the rest of the network before the blueprints are approved.

Similarly, IT’s involvement should be consistent and adaptive from building to building, and its requirements well articulated. IT should have final approval and inspect the plans and implementation to make sure it will meet the user's needs and be able to connect efficiently to the existing network and services.

Data Facilities

There are two parts to a data facilities design discussion. The first is the cloud concept, public or private, and the second is virtualization. Arguably a distinct part of cloud architecture, it is addressed separately so that specific design principles can be included.

Public Cloud

There are several advantages to a public cloud based architecture:

1. Going with a public cloud solution means that the organization does not need to manage a large and skilled team of technical (system, network, and facilities) administrators.
2. The underlying virtualization framework allows resources to be reallocated quickly and efficiently.
3. The ability to quickly upgrade by allocating additional hardware is very attractive for those services that are either experiencing extremely rapid growth or highly variable load. Examples of these would be a fast growing start-up delivering web-based services or a web presence for a short-duration but very popular event, such as the Olympics.

The downsides of a public cloud based architecture include:

1. One must ensure that services have been designed so that they may take advantage of the cloud solution. Example: If the core data path of an application is compute bound and single threaded, there may be no benefits in adding additional compute resources to that service.
2. One has now placed their data in someone else’s hands. It's difficult to ensure that for data with critical security requirements that they take this responsibility as seriously as the owner would like.
3. This service is farmed out to someone else who is trying to make a profit at providing this service. Consequently, any organization who has the expertise and facilities to provide such a service themselves has to balance the costs of paying the additional profit margin vs. the benefits accrued by gaining the provider's economies of scale.
4. In a public cloud, the services reside outside the campus network boundary. As we discuss in the next section, the notion of network perimeter is nebulous at best in this day
and age, but moving services outside of the core network certainly doesn't make protecting them in a holistic way any easier.

It is difficult to see how benefits number 1 and 3 apply to UNM, and we don't yet see how benefit 2 presents a pressing need. Consequently, we don't see a truly compelling benefit to moving services to the public cloud at the present time, although other external decisions could have an impact on this perception. Still, some services represent a lower risk than others. For example, non-secure email in the cloud can make an attractive proposition when considering the above risks and benefits.

Private Cloud

Regarding setting up a private cloud, disadvantage 1 (cited in the Public Cloud section above) still applies. In addition it requires significant expertise to properly manage server virtualization. (see Server Virtualization section below).

Server Virtualization

A large number of the organizations who start down the virtualization path don't wind up taking enough advantage of this architecture to have made the effort worthwhile. Setting up and running virtualized services effectively on a large scale requires a serious commitment and considerable expertise.

Virtualization provides benefit in a number of conditions. A non-exhaustive list includes:

- Space is at a premium
- Energy availability is at a premium
- Operational horsepower can be continually addressed
- Increased availability

There are downsides as well, just as in our discussion of cloud solutions above:

- Hardware failure can impact multiple services
- Performance can be impacted
- Difficulty in migration

The principle involved here is best dictated by the first of our design concepts: Conceptual Simplicity. While all of the concepts should be applied to any design principle, consider that in a virtualized world, these concepts are more dense.

Costs are often viewed as a significant benefit from virtualization. A large scale virtualization environment can lead to reduced cost that are the result of the benefits outlined above. However, if these other benefits are not realized, space, energy availability, and operation horsepower issues, then the additional expertise needed for meaningful virtualization can outweigh any benefit and actually increase costs.

Let us consider an abstract thought experiment about virtualization that highlights some of these advantages and disadvantages. Assume we chose to virtualize student registration. Obviously, the load on this service is greater right before and during the beginning of a semester.
Consequently, it is appealing to virtualize it and devote increased resources to it when they are necessary, and scale them back during non-peak periods.

However, what does this really accomplish? Are those resources really needed elsewhere outside the peak registration period? How do the costs of managing the virtualization process compare to the costs of just deploying this service on slightly more capable set of hardware and being done with it? In some environments, virtualization is a wonderful tool for delivering compute resources dynamically and efficiently. It’s easy, though, to get caught up in the elegance and not consider the real life cost/benefit ratio.

Virtualization should not be seen as an answer to a question that wasn’t asked. Keep in mind simplicity and flexibility. If the benefit of virtualization cannot be specifically articulated, it isn’t the correct answer.

**Migration**

Migration of any service, virtualized or otherwise is an important challenge to consider. And the starting point and target are not important aspects of the migration challenge (you can be going from one physical server to another, a physical to a virtual, from one virtual to another and these still apply).

Everything about a service must be understood. Not just the behavior of the service, but the technical aspects of the service. For example, service A is to be migrated from location X to location Y. For illustration purposes, let’s suppose that the two locations are in different buildings, behind different firewalls, going through different routers and switches. This might not be the case for any given service, but helps us illustrate the challenge.

Migration must consider what ports the service uses, what assets it connects with, how it interacts with the existing network architecture of location X and how, if at all, this will change at location Y. Any detail that is omitted will likely result in unwanted complexity in the migration process. If at all possible, the migration should be configured within the test bed first.

The UNM IT Services Building will need to be vacated at some point in the near future. While this is not a consideration for network design, it can be used as a convenient opportunity to migrate any services that may not yet be virtualized and are desired to be, or those simply needing to be migrated to a new location.

**Appropriate Security**

UNM is a diverse organization with diverse information security needs. IT security in an increasingly mobile world presents new challenges in order to adequately protect critical information resources. Securing a modern network is challenging, so solutions have to be simple and holistic.

Regardless of the disposition of an organization, its rules to access the assets or infrastructure of UNM, should be carefully defined and enforced. An organization, internal or external, can be made up of good actors. But a bad actor can corrupt a great deal if there are no effective controls. There are many contrite metaphors that say this in colorful ways. The reason there are so many is, it’s true.
Identity and Context

Identity is the one thing about a mobile and porous network that does not change. Identity aligns with authentication in the traditional AAA (authentication, authorization, and accounting) view of security, but principles for the future network need more than this traditional approach.

Historically, authentication and authorization are tied together, and these sorts of security approaches have shown their lack of flexibility. Fine grained access controls align with detailed authorization in the AAA view. Operating in an all or nothing mode, systems that employ fine grained authorization across the enterprise are typically so complex to operate in practice to be unacceptable, especially in an academic environment.

As ubiquity becomes a greater part of our porous and increasingly mobile network, an approach is needed that is more context aware and sensitive to the explicit and implicit demands on security and privacy. We’ll refer to this as an Identity Governance (Identity, Access Controls and Auditing) environment.

We may want physical location, time of day, authentication method, trust, access method, and other external conditions to influence what authentications and/or authorizations are granted. For example, it may be impermissible for a medical researcher to access patient information from networks outside the hospital’s control, but it might be okay to access research data or read email from anywhere. Doing this without identity and context awareness becomes a management and maintenance nightmare.

Another issue with traditional authentication or authorization solutions is how they are implemented, managed and used. One aspect of this, centralization vs decentralization, is often a touchy subject, but shouldn’t be in an Identity Governance environment.

In an Identity Governance environment, Identity (authentication) should be centralized, just as Human Resources is centralized. In this environment, authentication is nothing more than the identity of a person, server, service or device along with the method of authentication, conditions, external influence considerations and the trust we have in any of these.

Access Control (authorization) in an Identity Governance environment is the granting to an identity in the above context, access to an asset. It should be decentralized. This keeps the access control (authorization) functions under the control of those who are responsible for a given resource. There may be other elements of authorization that are out of the control of those responsible for a given resource such as firewall considerations for example.

Audit data of any identity use or access attempt is important, and it should be secured. Access to and storage of this data should also be centralized.

Selective Presentation

If a port doesn't have to be open or a service doesn't have to be run on a given computer, close it down. Default configurations should present a minimal network aspect. There are numerous standards that exist for this. One should be selected and implemented.
**Defense In Depth**

Creating an architecture with security measures only at the perimeter is not terribly effective under the best of circumstances, and in an academic environment such an effort is futile. Where should we draw the perimeter on the University network? Who is inside and who is outside? Clearly, this is very much dependent on the circumstances.

For critical information systems, the network on which they reside must be protected and monitored, the system itself must be protected and monitored, and access to the data (or any asset) itself should be restricted, monitored, and auditable, such as described in the *Identity and Context* section above.

While it may be tempting to simply trust access less from systems nearby than from those further away (in terms of network distance and relationship with those responsible for them), the truth is much more complex. Defense in depth means systems should be trusted as is strictly necessary, no more. While this ties directly to our *Identity and Context* section above, it stands alone as a key principle.

**Patch Efficiency**

Every security-conscious organization struggles under the perpetual cycle of vendor-issued security patches. A serious commitment of resources is necessary for the process of risk assessment and patch management for critical systems. There should be no task which could be assigned a higher priority for those who perform these updates.

For all systems if possible, but especially for those where downtime is particularly expensive, patches should be tested in the test environment, so that side effects may be measured for any given patch release.

The rollout system itself should be automated as much as is possible. Accounting of systems temporarily off the network, will ensure that these systems don't slip through the cracks.

In some cases, a service must be deployed in which the vendor retains access to the device(s) providing that service. Similarly, requirements may dictate that a system be supported that must run an obsolete and/or unpatched software version. In these cases, the network these services run on must be isolated from other networks in the same manner as if it were part of the Internet at large.

**Monitor and Audit**

Monitoring and auditing of authentication and authorization is covered in the *Identity and Context* section above. In this section we discuss the monitoring and auditing of network traffic itself. If one were to examine the network traffic traversing even a modestly open network, it would reveal amazing contents. While the ratio of bad actors to entities who are not a threat on the Internet may be small, the bad actors are awfully busy. We've all read the reports about how little time it takes for an unpatched computer hooked to the Internet to be successfully hacked. We also hear all about zero-day vulnerabilities and which organizations have had to issue very public non-apology apologies because they lost customer data.
Traffic monitoring harvests a huge amount of information. Determining a baseline for traffic on the networks that connect critical information systems to the Internet and investigating anomalies are not about repelling any particular attack, but about finding out in short order when they occur. As it turns out, while watching incoming connections to the critical services and attempted access without authorization will tell one something about your attackers, it's significant changes of data flows out of critical services that are the most reliable indicator of a malicious actor.

Remember, that from the perspective of protecting a network from these bad actors: there are an infinite number of holes to guard and an attacker need only find one.

**Next Steps**

Network users and designers should read, discuss and list any questions so that these principles and their concepts can be successfully applied to the design work which will follow. We look forward to the review of this document with other universities and working with UNM on the next steps in the design process.
Appendix A - VLAN Considerations

This appendix covers some of the more technical details of the problems with extensive VLAN use over a diverse network, such as UNM’s. Because the information here is more technical than the rest of the document we believe it is appropriate to split it out into a separate section. Those who aren't interested in detail regarding the difficulties in managing extensive virtual networks may safely skip this appendix.

The VLAN technology was initially designed to allow network engineers to virtually segment large bridged or switched 802.3 networks into subsets so that centrally located switches would not be overloaded and the total bandwidth of that network could be used more efficiently. By tagging traffic, different switches could be used to forward traffic from one segment of the larger physical network to another without creating loops or contributing to broadcast storms, which could bring down the entire network.

Later it was realized that this technology could be used in conjunction with larger than LAN switched networks to extend a LAN beyond its previous practical geographical boundaries. While this is convenient for those situations where two systems that must be both geographically distant and occupy the same logical network segment, this feature can easily be abused to create a network maintenance nightmare.

Here is an example of how this technology can be abused to turn a well ordered network into one that is inefficient and difficult to maintain. Let us suppose we have a campus ring network between four buildings, labeled A B C D, connected in that order, with buildings A and D also connected. Let us also assume that this is a switched network. We'll call this network the backbone.

Now, let us imagine that each of the buildings represented by a capital letter houses a network that we'll label by the respective lower case letter for that building. That is, building A is home to network a, etc.. Let us further assume that network a is connected to the backbone network by a router, located in building A of course, and likewise for all of the other building networks.

Now suppose someone's office is moved from building A to building B. Suppose further they had a requirement to still access printers in building A, and that the printing protocol in use didn't operate well across network boundaries. So, the network engineers connect the primary switch for network a up to the backbone network, and connect a port from the primary network switch in building B up to the backbone. Then they extend network a to the computer belonging to the person who needs access to it in building B by creating a VLAN, let's label it VLAN 101, between the two buildings.

Now let's imagine that there are two computers in building C (on network c) who perform an important function talking to each other via a broadcast protocol (which cannot operate beyond the boundary of the network). Due to resource constraints (power, space, whatever), it is determined that one of these machines must also be moved to building B, but since it needs to reside on network c to serve its function, the networking folks extend the VLAN that comprises...
network \( c \), let's call it VLAN 102, to the main switch in building B in the same manner as they did when extending network \( a \).

Now, what happens if the computers in building B that are on network \( c \) and network \( a \) wish to talk to each other? Well, if we start with the computer on network \( a \), the traffic must traverse VLAN 101 back to building A, then through the routed port of network \( a \) to the backbone, then on the backbone to building C, possibly passing back through building B, where it traverses the routed port to hop on VLAN 102, travels back to building B to the same primary switch for the building that it passed through initially, to get to the machine in that building on network \( c \).

In this example, the traffic traverses four backbone links and passes through the building B backbone switch at least twice and very possibly four times, each time heading in a different direction. This is an inefficient use of network bandwidth, switch and router capacity, and would be a nightmare to diagnose if some part of this connection goes wrong. Depending on how you choose to measure it, somewhere between half and all of the total backbone resources consumed on this transmission are wasted.

Of course, the premise for this scenario was that there were a set of machines that had to be on the same network segment as each other and had to move to a geographically distant location. Given these requirements, being able to extend those local networks using VLANs is incredibly convenient. However, the mess that this creates is now obvious.

In network engineering meetings all around the world, there are regular conversations that sound a lot like this:

Manager: "We have a requirement to directly connect some resource in one building with a resource in another building. How are we going to do this?"

Engineer: "Well, we could just extend the VLAN in the first building to the location of the resource in the second building?"

This seems like a simple solution to the problem, but it leads to a Gordian Knot of the sort described in the example in this section. In this conversation, someone should be saying, "Whoa there, while this sounds like an expedient solution to the problem, if this is something folks expect us to maintain for a while, we're making our network more complex and less maintainable, in the long run in order to knock this off our ToDo list right now. Maybe we should examine the requirements in more detail and see if there might not be some way to meet the needs of the customer without creating a long-term support problem for us?"

It's very tempting to exploit the flexibility of VLANs to quickly fix a whole host of networking requirements, but this should be resisted. Here are the circumstances where we feel extending VLANs across natural network boundaries are warranted:

- There is no other good technical method to connect the two resources (through proxies, by altering the communication protocol, or by having them use alternate resources).
- The need for this service is on a temporary basis (if the requester can't name an end date, it's not temporary).
- There is sufficient surplus bandwidth to accommodate the extra load.
The resource sitting on the extended portion of the VLAN will *not* be communicating with resources beyond its local network.

In our previous example, we didn't mention that the backbone network would almost certainly be implemented as VLAN itself. This is an exception to the rule since the VLAN in this case is the means for implementing a multi-building network with some redundancies. This is a different situation altogether and is not covered by our previous admonishments.

Finally, we note that a VLAN, such as the backbone VLAN in our example and the UNM campus VLAN(s), have some fault tolerance to component outages. If a network break occurs, the nodes that still have connectivity after the failure will be able to resume communication after the switches in question go through a process of re-architecting the network via one of a family of protocols known as spanning tree protocols. The problem is that these do not converge (repairing the network) quickly compared to routing protocols. The original Spanning Tree Protocol (STP) can take minutes to converge. Use of the updated Rapid Spanning Tree Protocol (RSTP) on the backbone, which typically converges in a few seconds. These convergence times depend on configuration settings, network complexity, and the type of failure.

Many services, such as email, won't be too adversely affected by an RSTP recalculation, but pseudo-realtime protocols, such as VOIP, streaming video, and the like, will be. The bottom line is that convergence times for switched networks using spanning tree protocols in the case of failure cannot be expected to be as fast as those for routing protocols. If the goal on a network, for example, the UNM core, is for near real-time convergence in the face of failure, routing is the way to go. A switched core network has the advantage that it provides more total throughput for the same cost, typically lower latencies, and it's easier to extend network segments across the core using VLANs.

Whether one deploys a switched or routed core depends entirely upon the cost/benefit calculation of these factors. Consequently, we can support either a switched or routed core network depending on how these various issues are weighted.