[Unit 6: Internet and Intranet Systems Development]
Internet Technology (CSC-402)

Jagdish Bhatta

Central Department of Computer Science & Information Technology
Tribhuvan University

Internet and Intranet Systems Development

Intranet:

Intranet is the generic term for a collection of private computer networks within an organization. An intranet uses network technologies as a tool to facilitate communication between people or work groups to improve the data sharing capability and overall knowledge base of an organization's employees.

Intranets utilize standard network hardware and software technologies like Ethernet, WiFi, TCP/IP, Web browsers and Web servers. An organization's intranet typically includes Internet access but is firewalled so that its computers cannot be reached directly from the outside.

Intranets are generally used for four types of applications:

1) Communication and collaboration:
- send and receive e-mail, faxes, voice mail, and paging
- discussion rooms and chat rooms
- audio and video conferencing
- virtual team meetings and project collaboration
- online company discussions as events (e.g., IBM Jams)
- inhouse blogs

2) Web publishing
- develop and publish hyperlinked multi-media documents such as:
- policy manuals, company newsletters
- product catalogs
- technical drawings
- training material
- telephone directories

3) Business operations and management
- order processing
- inventory control
- production setup and control
- management information systems
- database access

4) Intranet portal management

- centrally administer all network functions including servers, clients, security, directories, and traffic
- give users access to a variety of internal and external business tools/applications
- integrate different technologies
- conduct regular user research to identify and confirm strategy (random sample surveys, usability testing, focus groups, in-depth interviews with wireframes, etc.)

Benefits of intranet:

- **Workforce productivity**: Intranets can help users to locate and view information faster and use applications relevant to their roles and responsibilities. With the help of a web browser interface, users can access data held in any database the organization wants to make available, anytime and — subject to security provisions — from anywhere within the company workstations, increasing employees' ability to perform their jobs faster, more accurately, and with confidence that they have the right information. It also helps to improve the services provided to the users.

- **Time**: Intranets allow organizations to distribute information to employees on an *as-needed* basis; Employees may link to relevant information at their convenience, rather than being distracted indiscriminately by electronic mail.

- **Communication**: Intranets can serve as powerful tools for communication within an organization, vertically and horizontally. From a communications standpoint, intranets are useful to communicate strategic initiatives that have a global reach throughout the organization. The type of information that can easily be conveyed is the purpose of the initiative and what the initiative is aiming to achieve, who is driving the initiative, results achieved to date, and who to speak to for more information. By providing this information on the intranet, staff have the opportunity to keep up-to-date with the strategic focus of the organization. Some examples of communication would be chat, email, and or blogs.

- **Web publishing** allows cumbersome corporate knowledge to be maintained and easily accessed throughout the company using hypermedia and Web technologies. Examples include: employee manuals, benefits documents, company policies, business standards, news feeds, and even training, can be accessed using common Internet standards (Acrobat files, Flash files, CGI applications). Because each business unit can update the online copy of a document, the most recent version is usually available to employees using the intranet.

- **Business operations and management**: Intranets are also being used as a platform for developing and deploying applications to support business operations and decisions across the internetworked enterprise.

- **Cost-effective**: Users can view information and data via web-browser rather than maintaining physical documents such as procedure manuals, internal phone list and requisition forms. This can potentially save the business money on printing, duplicating documents, and the environment as well as document maintenance overhead.

- **Enhance collaboration**: Information is easily accessible by all authorised users, which enables teamwork.

- **Cross-platform capability**: Standards-compliant web browsers are available for Windows, Mac, and UNIX.

- **Built for one audience**: Many companies dictate computer specifications which, in turn, may allow Intranet developers to write applications that only have to work on one browser (no cross-browser compatibility issues). Being able to specifically address your "viewer" is a great advantage.

- **Promote common corporate culture**: Every user has the ability to view the same information within the Intranet.

- **Immediate updates**: When dealing with the public in any capacity, laws, specifications, and parameters can change. Intranets make it possible to provide your audience with "live" changes so they are kept up-to-date, which can limit a company's liability.

- **Supports a distributed computing architecture**: The intranet can also be linked to a company's management information system, for example a time keeping system.

Drawbacks of intranet

- it is an evolving technology that requires upgrades and could have software incompatibility problems
- security features can be inadequate
- inadequate system performance management and poor user support
- may not scale up adequately
- maintaining content can be time consuming
- some employees may not have PCs at their desks
- The aims of the organization in developing an intranet may not align with user needs

Protocols used in intranet systems:

An intranet uses the same concepts and technologies as the World Wide Web and Internet. This includes web browsers and servers running on the internet protocol suite and using Internet protocols such as FTP, TCP/IP, Simple Mail Transfer Protocol (SMTP) and so on.
Note: we have discussed all of these protocols already in previous units!!!

Intranet Network Infrastructure:

A network infrastructure is an interconnected group of computer systems linked by the various parts of a telecommunications architecture. **Specifically, this infrastructure refers to the organization of its various parts and their configuration — from individual networked computers to routers, cables, wireless access points, switches, backbones, network protocols, and network access methodologies.** Infrastructures can be either *open* or *closed*, such as the open architecture of the Internet or the closed architecture of a private *intranet*. They can operate over wired or wireless network connections, or a combination of both.

The simplest form of network infrastructure typically consists of one or more computers, a network or Internet connection, and a *hub* to both link the computers to the network connection and tie the various systems to each other. The hub merely links the computers, but does not limit data flow to or from any one system. To control or limit access between systems and regulate information flow, a switch replaces the hub to create network protocols that define how the systems communicate with each other. To allow the network created by these systems to communicate to others, via the network connection, requires a router, which bridges the networks and basically provides a common language for data exchange, according to the rules of each network.

Why Is the Network Infrastructure Important to Your Intranet?

An intranet is made up of two parts: **the applications (software / protocols) and the network infrastructure on which the applications run**. Applications— the visible part of an intranet —provide the functionality to improve productivity and lower costs. A wide spectrum of Internet/intranet applications is available from many vendors. **The network infrastructure includes the hardware—network interface cards (NICs), hubs, routers, switches, and servers—over which the applications run.** All network hardware is not the same, and an intranet is only as usable, reliable, and cost-effective as the hardware on which it runs. Crucial considerations in choosing appropriate hardware include:

- Bandwidth availability
- Reliability
- Value, in terms of both initial cost and ease of use and management
- Scalability, to ensure that present and future needs can be met

So as a part of network infrastructure, go through the above highlighted portions. I think you have studied those in data communication as well.

Intranet Implementation Guidelines:

When planning an intranet, there are a number of questions to be considered. These questions will set the tone for how you go about developing your intranet, help you establish guidelines.

1. What is your business case for building the intranet?
2. Who can publish to the intranet?
3. What types of content can be published?

Content Design, Development, Publishing and Management:

Content is a substance, and information on the site should be relevant to the site and should target the area of the public that the website is concerned with.

Content Management:

Content management, or **CM**, is the set of processes and technologies that support the collection, managing, and publishing of information in any form or medium. In recent times this information is typically referred to as content or, to be precise, digital content. Digital content may take the form of text (such as electronic documents), multimedia files (such as audio or video files), or any other file type that follows a content lifecycle requiring management. A critical aspect of content management is the ability to manage versions of content as it evolves

Content management is an inherently collaborative process. It often consists of the following basic roles and responsibilities:

- Creator - responsible for creating and editing content.
- Editor - responsible for tuning the content message and the style of delivery, including translation and localization.
- Publisher - responsible for releasing the content for use.
- Administrator - responsible for managing access permissions to folders and files, usually accomplished by assigning access rights to user groups or roles. Admins may also assist and support users in various ways.
- Consumer, viewer or guest- the person who reads or otherwise takes in content after it is published or shared.

A content management system is a set of automated processes that may support the following features:

- Import and creation of documents and multimedia material.
- Identification of all key users and their roles.

- The ability to assign roles and responsibilities to different instances of content categories or types.
- Definition of workflow tasks often coupled with messaging so that content managers are alerted to changes in content.
- The ability to track and manage multiple versions of a single instance of content.
- The ability to publish the content to a repository to support access to the content. Increasingly, the repository is an inherent part of the system, and incorporates enterprise search and retrieval.

Intranet Design with Open source Tools: DRUPAL, JUMLA:

Druple:

Drupal content management system or Drupal CMS is an open source modular framework and Content Management System written in PHP that can be used to manage your website or blog from an online interface. Drupal is used as a "back end" system for many different types of websites; ranging from a small personal blog to large corporate sites. It allows an individual or a community of users to easily publish, manage and organize a wide variety of content on a website.

Joomla:

Joomla CMS is a web application that makes it easy for any person to build a website. A website created with custom Joomla design allows the user to take control of their website. The beauty of Joomla is that the designers can leverage the existing framework and user interface to deliver applications to the end users in a familiar, powerful environment. This process saves time as well as cuts the budget down.

Tunneling Protocols:

A tunneling protocol is the one utilized by computer networks in cases where the network protocol or the delivery protocol encapsulates an unsuited payload protocol at a peer level or lower than it. The protocol is termed as such because this appears as if it makes its way through the various types of packets. It is sometimes recognized with the name “encapsulation protocol” but this label is very vague for the reason that there are other network protocols which are also designed to perform the process of encapsulation.

Tunneling protocol is widely used in transmitting large amounts of protocols through the typical networks. In addition, it may serve as a medium for transferring virtual private networks (VPNs) that are already encrypted.

This protocol comes as an advantage since tunneling may be employed in transporting a payload over the mismatched delivery-network. Tunneling protocol is also helpful when it comes to presentation of a safe passageway over a suspicious-looking network.

In common cases, tunneling may differ with some other forms of layered protocol including TCP/IP and OSI. There are times when a delivery protocol functions at a more advanced level in the model compared to that of a payload protocol. Rarely, however, does both the delivery and payload protocol work at similar level.

Wrapping of protocols is a product of the mechanism performed by the conventional layered protocols. This works in line with the other models such as the OSI model and TCP/IP model, which does not belong in the category of protocols that carry out tunneling. There are different procedures that may be employed by these tunneling protocols so as to do its job successfully. One of which is the utilization of data encryption for the purpose of transferring a vulnerable payload protocol through a public network, in which the most common type is the Internet. Lastly, this process solely offers the functionality of the VPN.

Different types of VPN tunneling:

Two types of tunneling include voluntary and compulsory.

- **Voluntary VPN tunneling:** In this particular tunneling type, the VPN client sets up the connection. At first, the client establishes a connection with the network provider or the ISP. Later on, utilizing this live connection, it creates a tunnel to a particular VPN server.

- **Compulsory VPN tunneling:** The carrier network provider is responsible for managing the set up for VPN connection in this type of tunneling. It is quicker than its voluntary counterpart and can be established in just a single step as compared to the two-step process of the other one. This network device is known with varied other names as well such as Network Access Server (NAS), VPN Front End Processor (FEP) and Point of Presence Server (POS).

Example of VPN Tunneling:

The following steps illustrate the principles of a VPN client-server interaction in simple terms;

Assume a remote host with public IP address 1.2.3.4 wishes to connect to a server found inside a company network. The server has internal address 192.168.1.10 and is not reachable publicly. Before the client can reach this server, it needs to go through a VPN server / firewall device that has public IP address 5.6.7.8 and an internal address of 192.168.1.1. All data between the client and the server will need to be kept confidential; hence a secure VPN is used.

1. The VPN client connects to a VPN server via an external network interface.
2. The VPN server assigns an IP address to the VPN client from the VPN server's subnet. The client gets internal IP address 192.168.1.50, for example, and

creates a virtual network interface through which it will send encrypted packets to the other tunnel endpoint (the device at the other end of the tunnel). (This interface also gets the address 192.168.1.50.)

3. When the VPN client wishes to communicate with the company server, it prepares a packet addressed to 192.168.1.10, encrypts it and encapsulates it in an outer VPN packet, say an IPSec packet. This packet is then sent to the VPN server at IP address 5.6.7.8 over the public Internet. The inner packet is encrypted so that even if someone intercepts the packet over the Internet, they cannot get any information from it. They can see that the remote host is communicating with a server/firewall, but none of the contents of the communication. The inner encrypted packet has source address 192.168.1.50 and destination address 192.168.1.10. The outer packet has source address 1.2.3.4 and destination address 5.6.7.8.
4. When the packet reaches the VPN server from the Internet, the VPN server unencapsulates the inner packet, decrypts it, finds the destination address to be 192.168.1.10, and forwards it to the intended server at 192.168.1.10.
5. After some time, the VPN server receives a reply packet from 192.168.1.10, intended for 192.168.1.50. The VPN server consults its routing table, and sees this packet is intended for a remote host that must go through VPN.
6. The VPN server encrypts this reply packet, encapsulates it in a VPN packet and sends it out over the Internet. The inner encrypted packet has source address 192.168.1.10 and destination address 192.168.1.50. The outer VPN packet has source address 5.6.7.8 and destination address 1.2.3.4.
7. The remote host receives the packet. The VPN client unencapsulates the inner packet, decrypts it, and passes it to the appropriate software at upper layers.

Overall, it is as if the remote computer and company server are on the same 192.168.1.0/24 network.

Tunneling protocols for VPN:

Five prominent tunneling protocols are readily used to establish successful VPN connection that includes **PPTP VPN**, **L2TP VPN**, **IPSec**, **SSH VPN** and **SSTP VPN**. Let us discuss them in brief.

- **Point-to-Point Tunneling Protocol (PPTP):** It is among the most widely preferred tunneling protocols and is available as a built in facility in almost all the windows OS versions. It utilizes a control channel over TCP to encapsulate PPP data packets. It itself does not provide authentication or encryption features but is dependent on the Point-to-Point Protocol (PPP). Still, it is the best to provide high security level and remote access during a VPN connection.

- **Layer 2 Tunneling Protocol** (**L2TP**): It is also a capable tunneling protocol that supports VPN connection. Like PPTP, it also does not offer confidentiality and

encryption on its own but depends on an encryption protocol for the same that it leverages to assure privacy within the tunnel. It has been developed out of the combination of L2F and PPTP taking their best features and exists at the data link layer in the OSI model, same as PPTP.

- **IP Security (IPSec):** It is better known as an assemblage of varied protocols instead of being a single one. When combines with PPTP or L2TP, it provides accomplished encryption solutions and secures the data transfer within a VPN tunnel. It exists at the Layer 3, i.e. Network Layer of the OSI model.

- **Secure Shell (SSH):** This is a new protocol as compared all the rest ones and seeks assistance of an encrypted channel to transfer the unencrypted data via a secure network efficiently. In locations where VPN is blocked, SSH somehow manages to hide the identity of users and prevents their IP address from being blocked.

- **Secure Socket Tunneling Protocol:** This is yet another effective protocol that makes way for secure data transfer from network server to a remote terminal and vice versa, thereby bypassing all the firewalls and web proxies coming in its way. To accomplish such a successful data transaction, it utilizes HTTPs protocol and is very useful at places where PPTP or L2TP/IPSec cease to perform as per expected.