Chapter 6

Internet and Intranet Systems Development

By Pavan Poudel

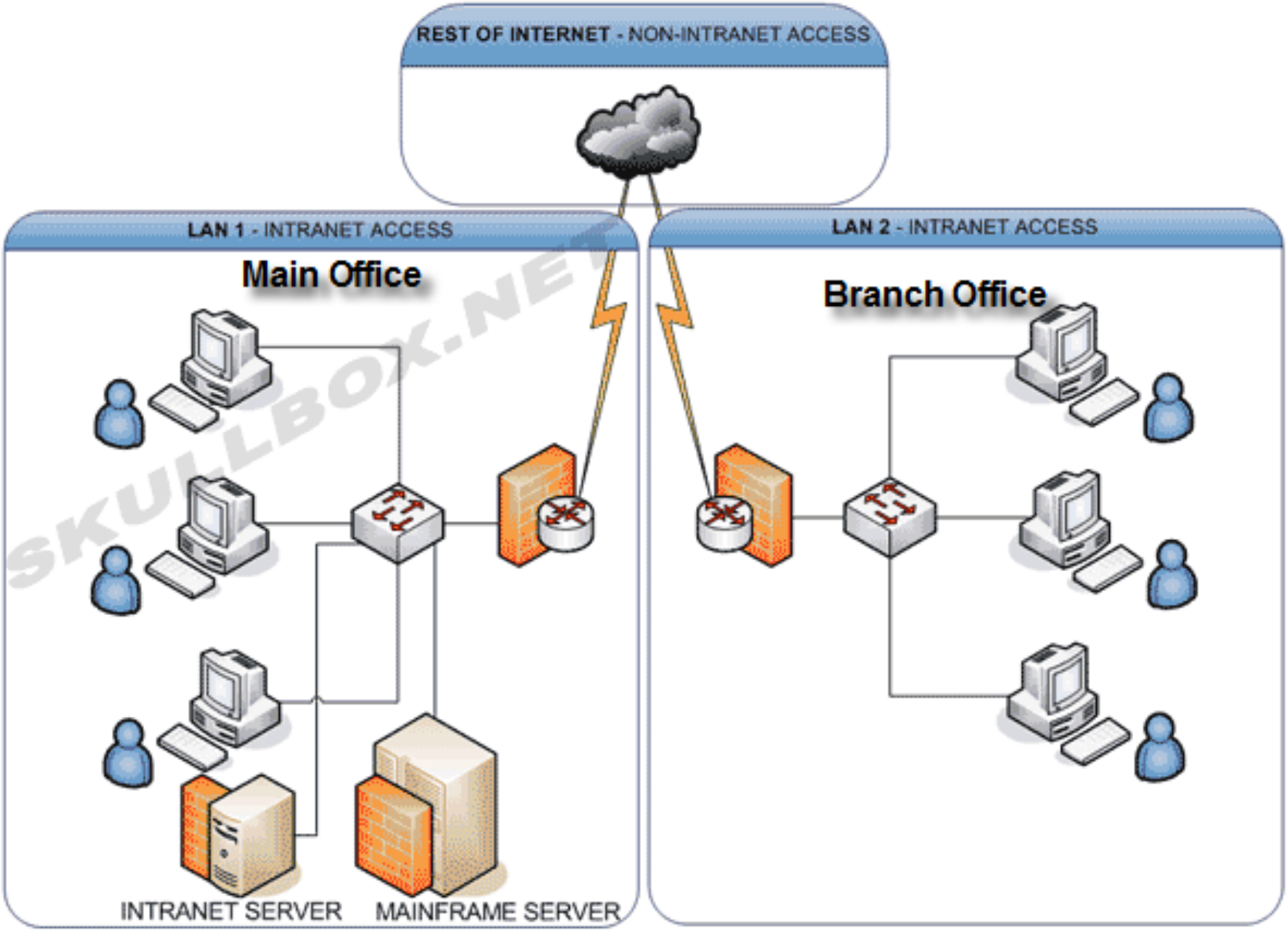
Overview

1. Introduction
2. Benefits and Drawbacks of Intranets
3. Intranets Implementation Guidelines
4. Intranet Resource Assessments: Network Infrastructure, Client and Server Resources
5. Content Design, Development, Publishing and Management
6. Intranets Design with Open Source Tools: Wordpress, Joomla, Drupal
7. Tunneling Protocols: VPN

Intranet

- An intranet is a private network that is contained within an enterprise.
- It may consist of many interlinked local area networks and also use leased(paisa terera line liney) lines in the wide area network.
- Typically, an intranet includes connections through one or more gateway computers to the outside Internet.
- The main purpose of an intranet is to share company information and computing resources among employees.
- An intranet can also be used to facilitate working in groups and for teleconferences.
- An intranet uses TCP/IP, HTTP, and other Internet protocols and in general looks like a private version of the Internet.
- With tunneling, companies can send private messages through the public network, using the public network with special encryption/ decryption and other security safeguards to connect one part of their intranet to another.

Intranet


REST OF INTERNET - NON-INTRANET ACCESS
LAN 1 - INTRANET ACCESS
Main Office
LAN 2 - INTRANET ACCESS
Branch Office
INTRANET SERVER
MAINFRAME SERVER

Advantages of Intranet

- **Intranets offering workforce productivity**
  - find and observe information very fast
  - use applications according to their roles and tasks
  - Through web browser a user can get access to entire contents of intranet website from anywhere or any time
  - also increase the ability of employee's by performing their job confidently very fast, and accurately
- **Time**
  - 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 email.
- **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

Advantages of Intranet

- **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
- **Enhance collaboration**
  - Information is easily accessible by all authorized users, which enables teamwork.
- **Cross-platform capability**
  - Standards-compliant web browsers are available for Windows, Mac, and UNIX
- **Immediate updates**
- **Supports a distributed computing architecture**:
  - The intranet can also be linked to a company's management information system, for example a time keeping system.
- **Multiple Branches which are geographically located can be connected.**

Disadvantages of Intranet

- **Intranet** has great features for interconnected manners but has some **disadvantages** too.
- Management does need to stop control of specific information, this problem can be minimized but with appropriate prudence.
- The other disadvantage of Intranet is security issue.
- Intranet gathered everything in one location which is really good but if it is not prearranged then you will spoil everything.
- The cost of intranet is very high but has lots of advantages after implementation.

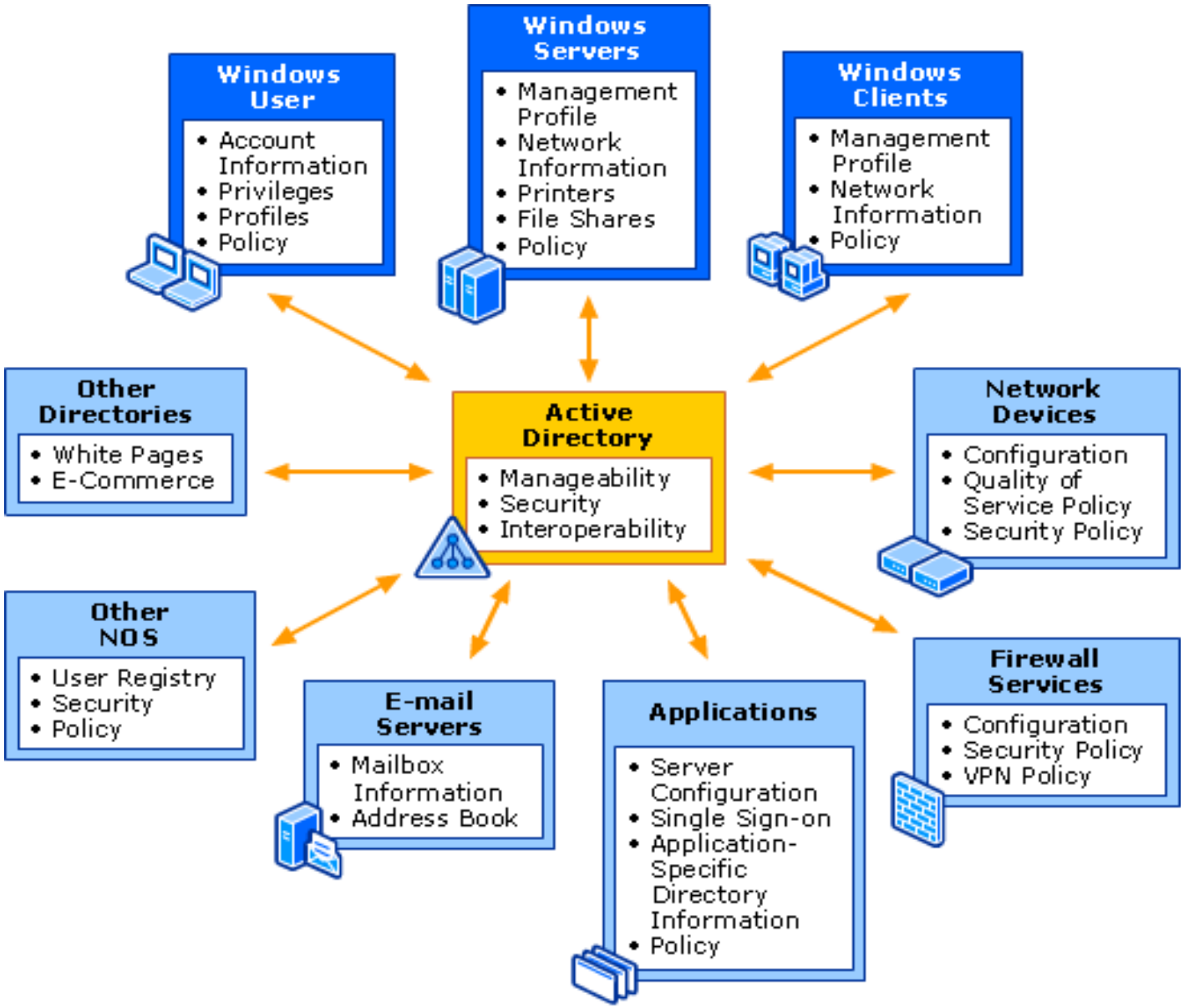
Disadvantages of Intranets

Management concerns	❑ Management fears loss of control ❑ Hidden or unknown complexity and costs ❑ Potential for chaos
Security concerns	❑ Unauthorized access ❑ Abuse of access ❑ Denial of service ❑ Packet sniffing
Productivity concerns	❑ Overabundance of information ❑ Information overload lowers productivity ❑ Users set up own web pages

Protocols used in Intranet

- HTTP(s)
- SMTP(s)
- IMAP(s)
- POP3(s)
- DHCP
- DNS
- FTP
- SSH
- VOIP
- Active Directories or LDAP (Lightweight Directory Access Protocol)
- VPN
- Some kind of indexing and searching service

Active Directory Services



Intranet Implementation Guidelines

- In order to develop a well structured and organized intranet that would fulfill all requirements, one would have to follow the right intranet development guidelines.
- Before starting developing intranet, one need to do extensive research and an in-depth needs analysis to find out what exactly your requirements are and what you want to achieve.
- The intranet development guidelines will help and guide during the different stages of the development process.
  - The purpose and goals of the intranet
  - Persons or departments responsible for implementation and management
  - Functional plans, information architecture, page layouts, design
  - Implementation schedules and phase-out of existing systems
  - Defining and implementing security of the intranet
  - How to ensure it is within legal boundaries and other constraints
  - Level of interactivity (e.g. wikis, on-line forms) desired.
  - Is the input of new data and updating of existing data to be centrally controlled or devolved

Intranet Implementation Guidelines

Actual Intranet Implementation Includes:

- Securing senior management support and funding.
- Business requirements analysis.
- Identify users' information needs.
- Installation of web server and user access network.
- Installing required user applications on computers.
- Creation of document framework for the content to be hosted.
- User involvement in testing and promoting use of intranet.
- Ongoing measurement and evaluation, including through benchmarking against other intranets

Intranet Resource Assessment

- Network Infrastructure
  - Your network infrastructure is the underlying foundation of the system. It forms the services that create the operating makeup of your network.
    - Understanding Your Existing Network
    - Understanding Network Infrastructure Components
    - Planning Your Network Infrastructure Layout
- Client server resources

Understanding your existing network

- Physical communication links, such as cable length, grade, and so forth.
- Communication links, such as analog, ISDN, VPN, and so forth, and available bandwidth and latency between sites
- Server information, including:
  - Host names
  - IP addresses
  - Domain Name System (DNS) server for domain membership
- Locations of devices on your network, including:
  - Hubs
  - Switches
  - Modems
  - Routers and bridges
  - Proxy servers
- 5. Number of users at each site, including mobile users

Understanding network infrastructure components

- The following common network infrastructure components have a direct impact upon the success of your deployment:
  - Routers and switches
  - Firewalls
  - Load balancers
  - Storage Area Network (SAN)
  - DNS

Planning your network infrastructure layout

- In deriving your infrastructure topology, you need to consider the following perspectives:
  - DMZ (Demilitarized Zone)
  - Intranet
  - Internal Network
  - Proxies

Intranet Sites Development

- An Intranet is a private network that uses common web technology for use within an enterprise or organization.
- Access to the network is restricted.
- Intranets may serve anything from small workgroups sharing the same office space to entire corporation with locations around globe.
- Intranet applications are typically used in “Business to Employee” (B2E) context, which means they are used to communicate with employees and share information within the organization.
- A **content management system (CMS)** is software that keeps track of every piece of content on Web site, much like local public library keeps track of books and stores them.
- Content can be simple text, photos, music, video, documents, or just about anything you can think of.
- A major advantage of using a CMS is that it requires almost no technical skill or knowledge to manage. Since the CMS manages all content, one don't have to.

Intranet Development with Open Source Tools

- Wordpress
- Joomla
- Drupal

Wordpress

- **WordPress** is a free and open source blogging tool and a content management system (CMS) based on PHP and MySql, which runs on a web hosting service and licensed under the GPLv2 .
- **WordPress** is web software you can use to create a beautiful website or blog.
- WordPress is an Open Source project, which means there are hundreds of people all over the world working on it. It also means you are free to use it for anything without paying anyone a license fee and a number of other important freedoms.

Wordpress

- Features of wordpress:
  - Themes

    WordPress users may install and switch between Themes. Themes allow users to change the look and functionality of a WordPress website or installation without altering the information content or structure of the site.
  - Plugins

    The plugin architecture allows users and developers to extend its abilities beyond the core installation.
  - Multi-user and multi-blogging
  - Mobile view support

Drupal

- Drupal is open source software maintained and developed by a community of 630,000+ users and developers.
- It's distributed under the terms of the GNU General Public License (or "GPL"), which means anyone is free to download it and share it with others.
- This open development model means that people are constantly working to make sure Drupal is a cutting-edge platform that supports the latest technologies that the Web has to offer.
- The Drupal project's principles encourage modularity, standards, collaboration, ease-of-use, and more.

Who's using Drupal ?

From local businesses to global corporations, diverse organizations use Drupal.

- News Publishing
  NowPublic, Popular Science, Economist
- Intranet/Corporate Websites
  AOL Corporate, Dahon Bicycles
- Education
  San Jose State University, Harvard, MIT, Council on Writing Program Administrators
- Art, Music, Multimedia
  MTV UK, Sony Music, Warner Brothers Records
- Community Portal Sites
  Fast Company, Team Sugar, Ubuntu Brainstorm
- Social Networking Sites
  DrupalSN

Joomla

- Joomla is content management system (CMS), which enables to build Web sites and powerful online applications.
- Many aspects, including its ease-of-use and extensibility, have made Joomla the most popular Web site software available.
- Best of all, Joomla is an open source solution that is freely available to everyone.
- Joomla is used all over the world to power Web sites of all shapes and sizes. For example:
  - Corporate Web sites or portals
  - Corporate intranets and extranets
  - Online magazines, newspapers, and publications
  - E-commerce and online reservations
  - Government applications
  - Small business Web sites
  - Non-profit and organizational Web sites
  - Community-based portals
  - School and church Web sites
  - Personal or family homepages

Joomla

Here are just a few examples of Web sites that use Joomla:

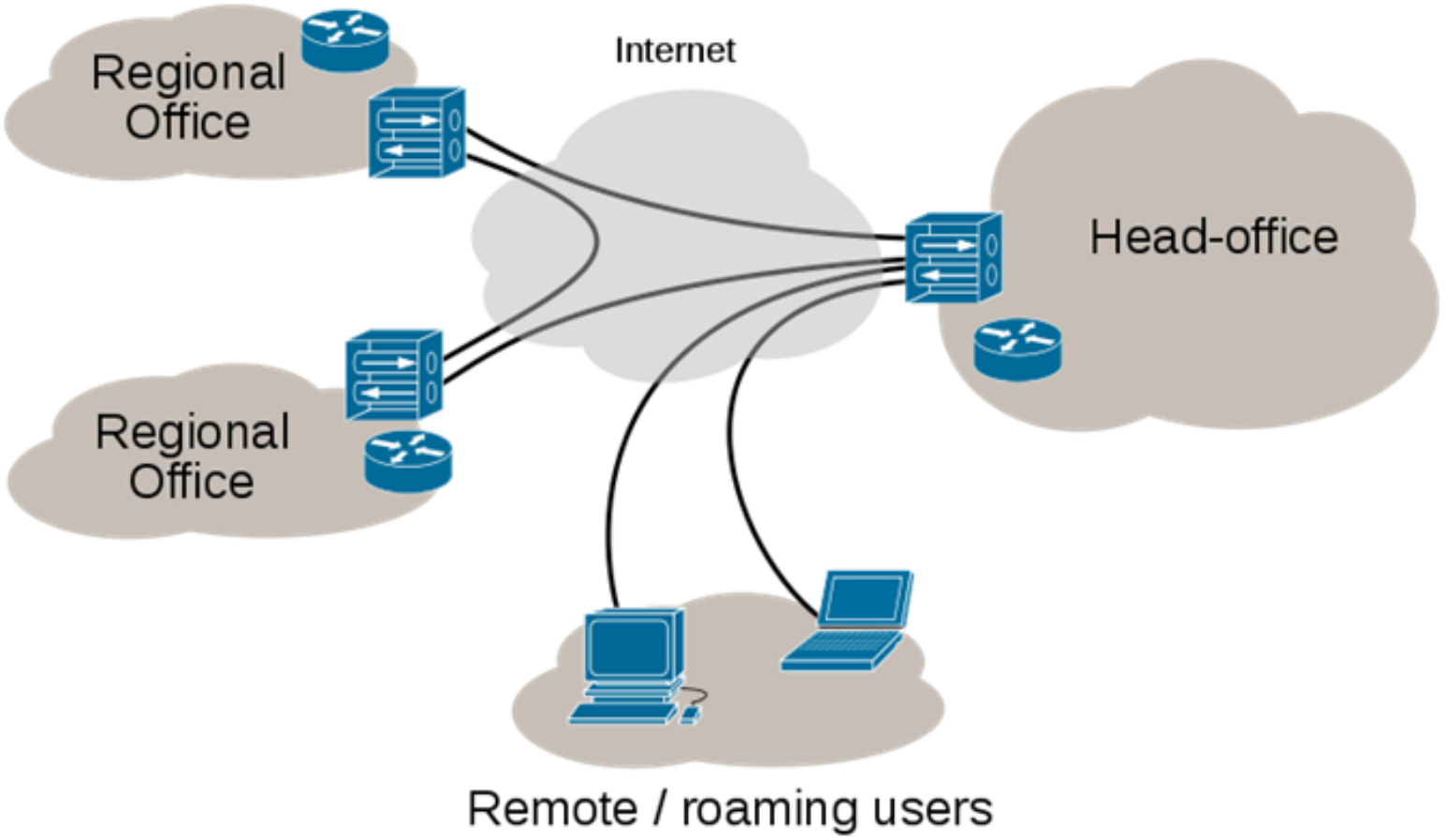
- MTV Networks Quizilla (Social networking) - http://www.quizilla.com
- IHOP (Restaurant chain) - http://www.ihop.com
- Harvard University (Educational) - http://gsas.harvard.edu
- Citibank (Financial institution intranet) - Not publicly accessible
- The Green Maven (Eco-resources) - http://www.greenmaven.com
- Outdoor Photographer (Magazine) - http://www.outdoorphotographer.com
- PlayShakespeare.com (Cultural) - http://www.playshakespeare.com
- Senso Interiors (Furniture design) - http://www.sensointeriors.co.za

Virtual Private Network

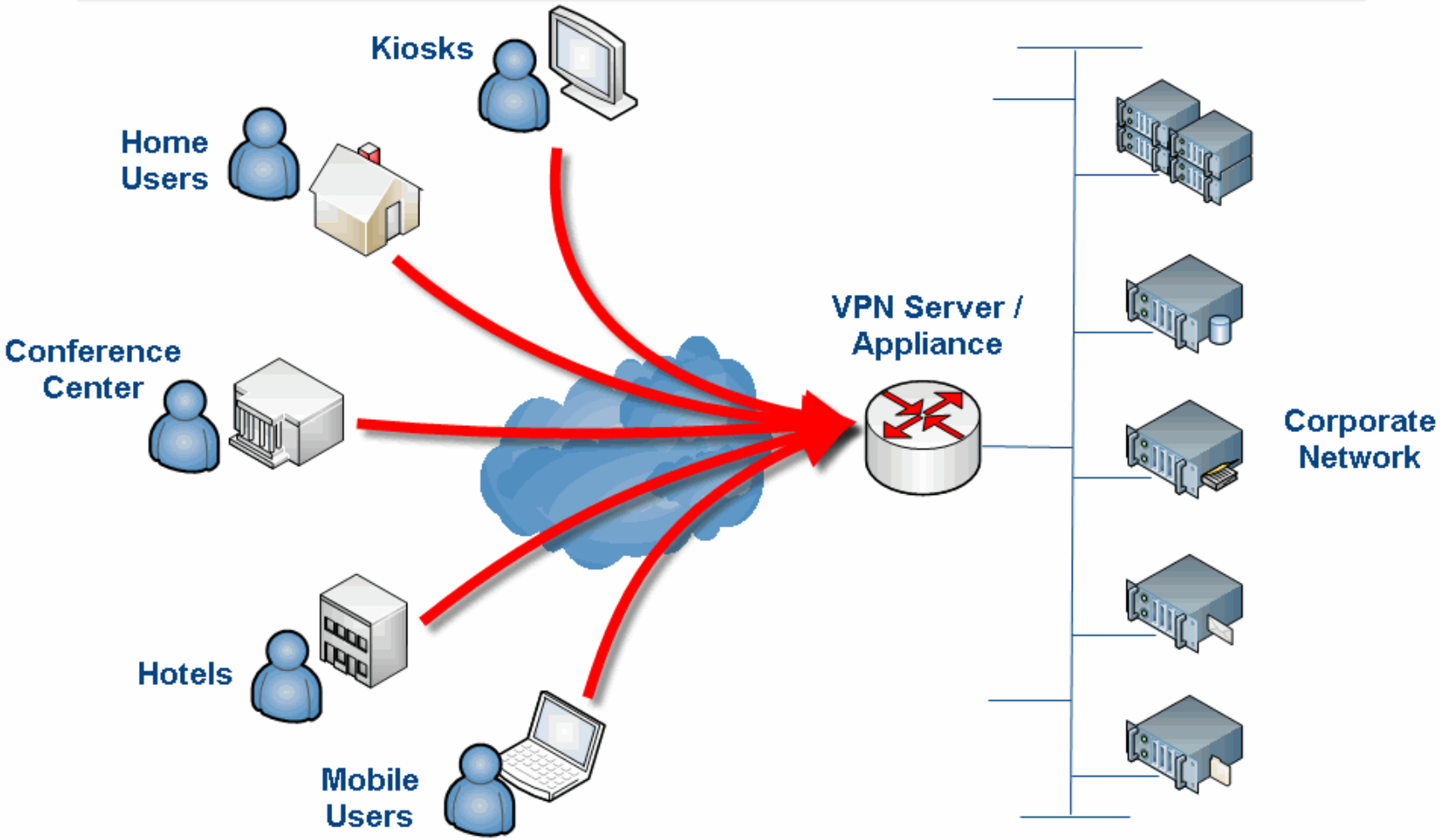
- A virtual private network (VPN) is a private network that interconnects remote (and often geographically separate) networks through primarily public communication infrastructures such as the Internet.
- It enables a computer to send and receive data across shared or public networks as if it is directly connected to the private network.
- A VPN is created by establishing a virtual point-to-point connection through the use of either dedicated connection, or virtual tunneling protocols, or traffic encryptions.
- Through VPN, you can access your private network over internet.
- VPNs provide security through tunneling protocols and security procedures such as encryption. For example, a VPN could be used to securely connect the branch offices of an organization to a head office network through the public Internet.

Virtual Private Network

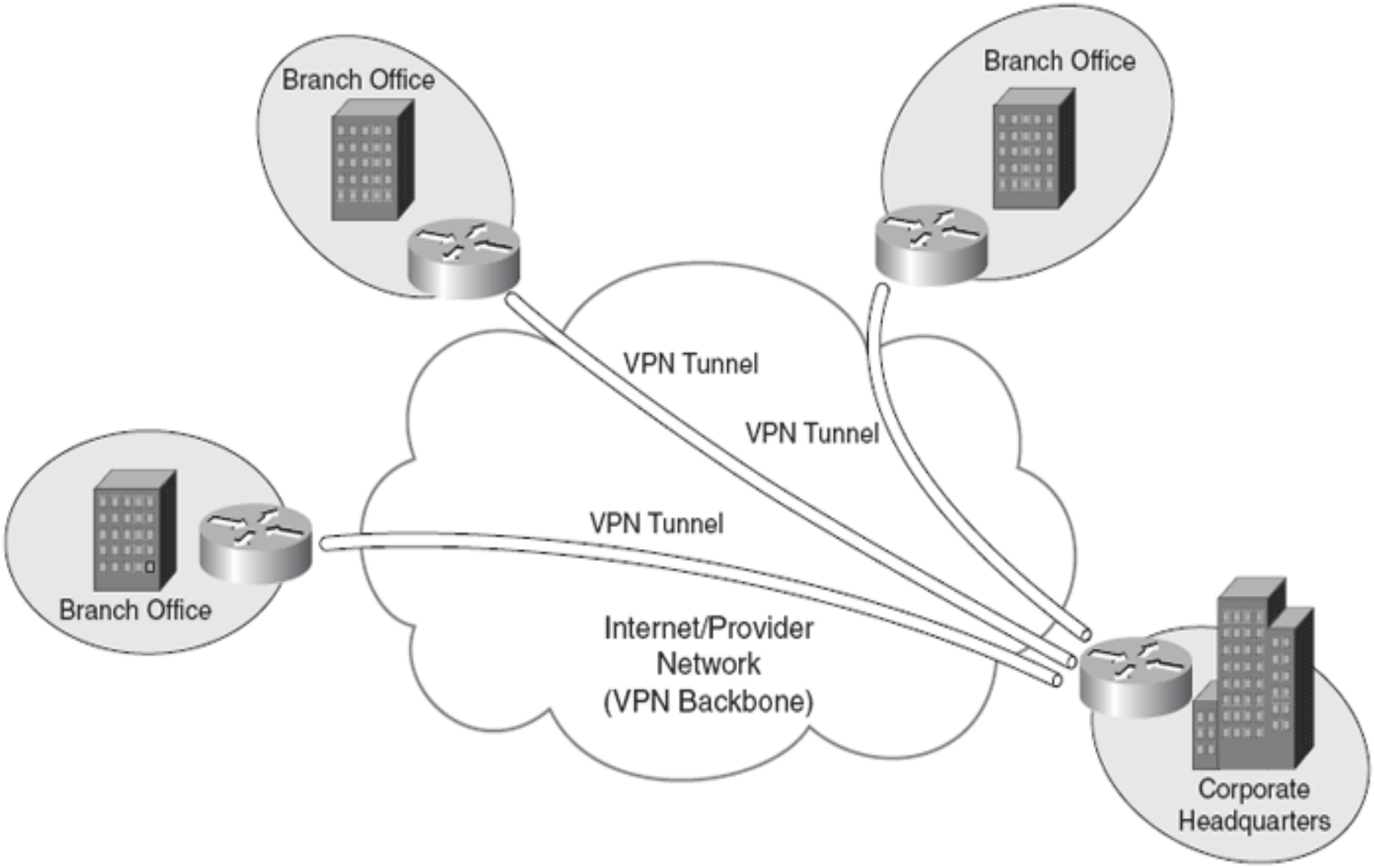
- Host to Gateway/remote-access VPNs and
- Gateway to Gateway/Site to Site VPN



Remote Access VPN



Site to Site VPN



VPN

- VPNs allow employees to securely access their company's intranet while traveling outside the office.
- Similarly, VPNs securely connect geographically disparate offices of an organization, creating one cohesive network.
- VPN technology is also used by Internet users to connect to proxy servers for the purpose of protecting personal identity and location.

IP Security(IPSec)

- **Internet Protocol Security** (**IPsec**) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
- IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks.
- IPsec can be used in protecting data flows between a pair of hosts (*host-to-host*), between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).
- Two principal protocols
  - **Authentication Header (AH) protocol** and
  - **Encapsulation Security Payload (ESP) protocol**

IP Security(IPSec)

- When a source host sends secure datagrams to a destination host, it does so with either the AH protocol or with the ESP protocol.
- The AH protocol provides source authentication and data integrity but does not provide secrecy.
- The ESP protocol provides data integrity and secrecy. Providing more services, the ESP protocol is naturally more complicated and requires more processing than the AH protocol.

IPSec elements

IPSec contains the following elements:

- **Encapsulating Security Payload (ESP)**: Provides confidentiality, authentication, and integrity.
- **Authentication Header (AH)**: Provides authentication and integrity.
- **Internet Key Exchange (IKE)**: Provides key management and Security Association (SA) management.

IPSec Security Features

- IPSec is the most secure method commercially available for connecting network sites. IPSec was designed to provide the following security features when transferring packets across networks:
- **Authentication:** Verifies that the packet received is actually from the claimed sender.
- **Integrity:** Ensures that the contents of the packet did not change in transit.
- **Confidentiality:** Conceals the message content through encryption.

Thank You !!!