

Designing and Implementing a Secure Network Infrastructure

NANOG October 19, 2003

Merike Kaeo

kaeo@merike.com

Agenda

- **Session I (1:30 – 3:00)**
Security Technology Details
- **Session II (3:30 – 5:00)**
Secure Infrastructure Architectures
- **Session III (7:30 – 9:00)**
Sample Configuration Scenarios

Security Technology Details

Who cares about technology if
you don't know what you want
or need to protect.....

First Step.....Security Policy

- What are you trying to protect?
 - What data is confidential?
 - What resources are precious?
- What are you trying to protect against?
 - Unauthorized access to confidential data?
 - Malicious attacks on network resources?
- How do regulatory issues affect your policy?

Characteristics of a Good Security Policy

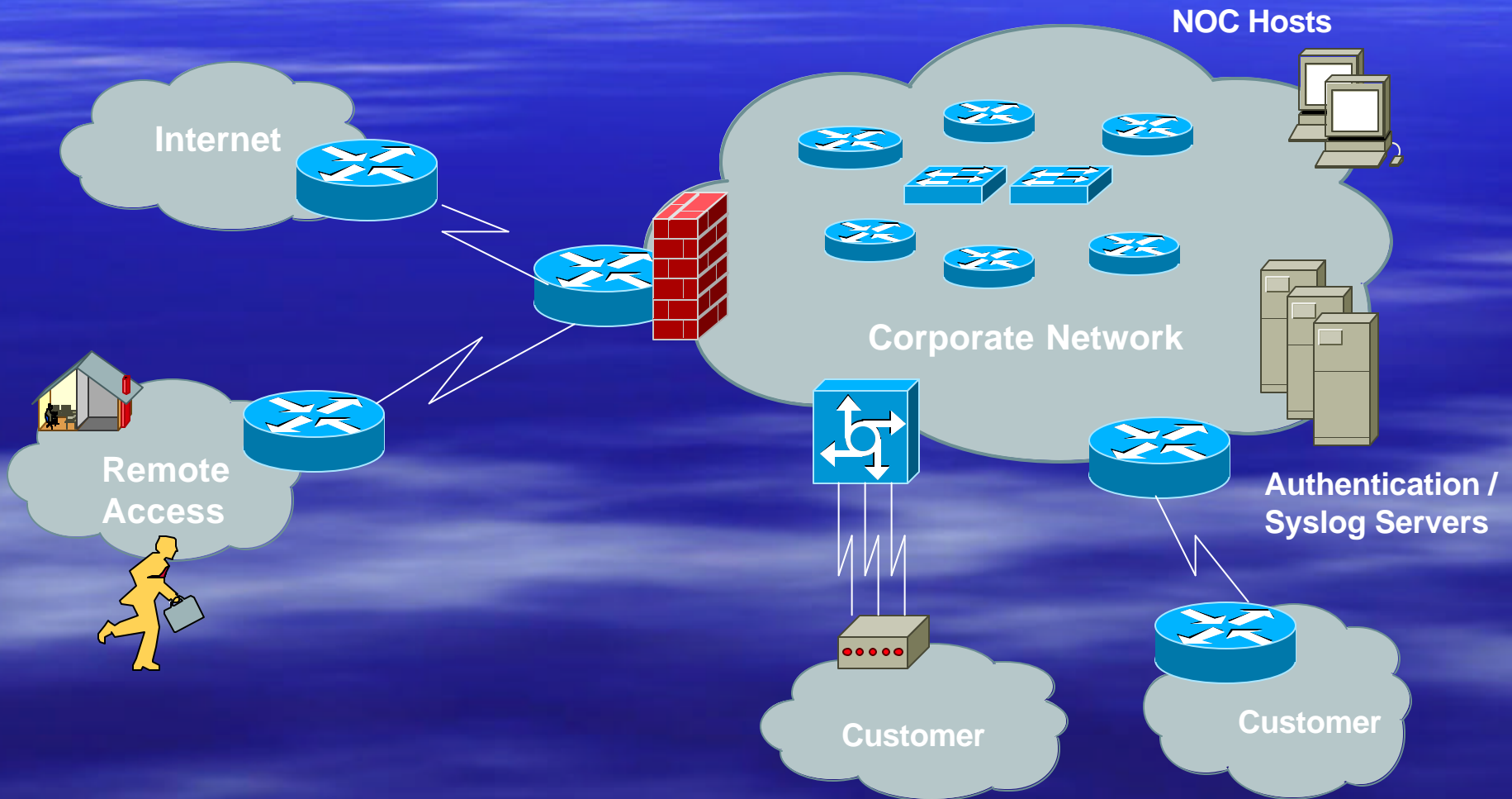
- Can it be implemented technically?
- Are you able to implement it organizationally?
- Can you enforce it with security tools and /or sanctions?
- Does it clearly define areas of responsibility for the users, administrators, and management?
- Is it flexible and adaptable to changing environments?

Why Should You Care?

- Your job may be at stake
- Your reputation may be at stake
- Why do you **not** care?

Time for reality check.....most companies **STILL DO NOT** have corporate sanctioned security policies....operators define them ad-hoc

Typical Network Components



Elements of a Security Architecture

- Authentication
- Authorization
- Data Integrity
- Data Origin Authentication
- Data Confidentiality
- Network Availability
- Audit

Questions To Ask

- Who can have access to what?
- How to provide authentication?

- Physical device security?
- Device network access security?
- Need for data confidentiality?
- Need for data integrity?

- How to verify security policy?
- How to enforce policy?
- How to detect intrusions?

Varying Degrees of Robustness for Security Elements

Will I Go Bankrupt ?



- Spend More Money
- Spend More Time

Is It An Embarrassment ?

NEED TO DO A RISK ANALYSIS !

Risk Assessment

- Identify critical assets
 - Hardware, software, data, people, documentation
- Place a value on asset
 - Intangible asset – importance or criticality
 - Tangible asset – replacement value and/or training costs
- Determine likelihood of security breaches
 - What are threats and vulnerabilities?

Risk Mitigation vs Cost of Security

Risk mitigation: the process of selecting appropriate controls to reduce risk to an acceptable level.

The ***level of acceptable risk*** is determined by comparing the risk of security hole exposure to the cost of implementing and enforcing the security policy.

Assess the cost of certain losses and do not spend more to protect something than it is actually worth.

The Security Policy Should Include.....

- Physical security controls
 - Media
 - Equipment location
 - Environmental safeguards
- Logical security controls
 - Subnet boundaries
 - Routing boundaries
 - Logical access control (preventative / detective)
- System and data integrity
 - Firewalls
 - Network services
- Data confidentiality

The Security Policy Should Include....

- Mechanisms to verify and monitor security controls
 - Accounting
 - Management
 - Intrusion detection
- Policies and procedures for staff that is responsible for the corporate network
 - Secure backups
 - Equipment certification
 - Use of Portable Tools
 - Audit Trails
 - Incident Handling
- Appropriate security awareness training for users of the corporate network

Incident Handling

- You will have to deal with a security breach
- Software will always require upgrades due to vulnerability discovery
- DON'T PANIC

Have procedures in place before a security breach happens!!!

Useful Resources

- <http://www.ietf.org>
- <http://www.sans.org>
- <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/default.asp>
- <http://www.robertgraham.com/pubs/network-intrusion-detection.html>

Security Policy Summary

- Need to have a comprehensive document for legal support
- Need a companion document which all corporate users will actually read

Security Technology Fundamentals

- **Crypto 101**
- Authentication Technologies
- Application Layer Security
- Transport Layer Security
- Network Layer Security (IPsec)
- Link Layer Security

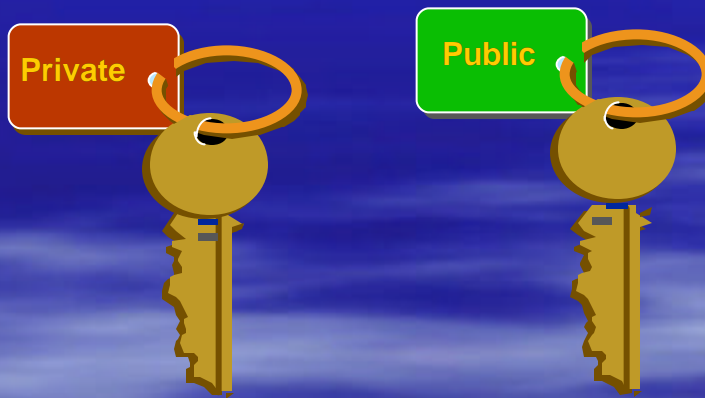
Cryptography Is Used For ?

- Authentication Protocols
- Data Origin Authentication
- Data Integrity
- Data Confidentiality

Public Key Encryption

Uses public/private keys

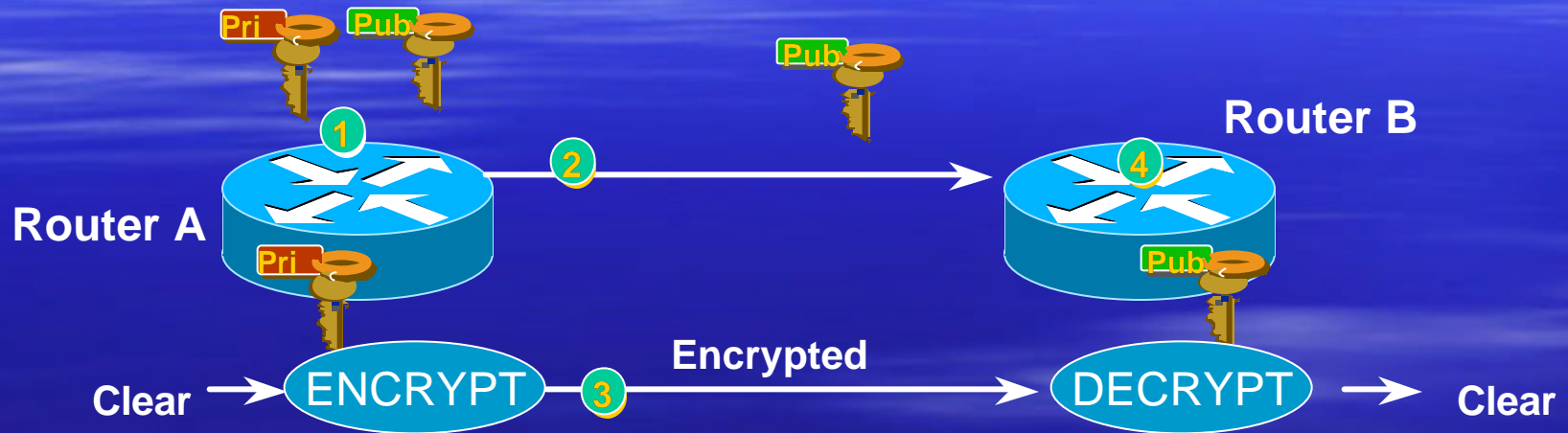
- Keep private key private
- Anyone can see public key



Computing Key pair is computationally expensive!!

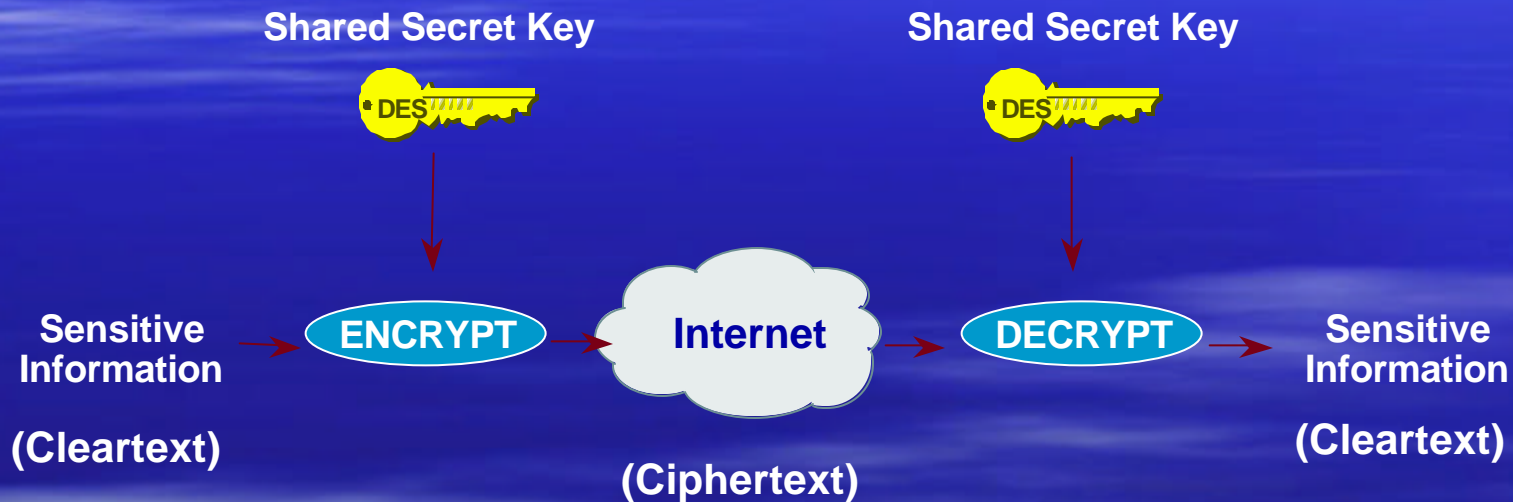
Common Algorithms: RSA, El Gamal

Data Origin Authentication



1. Router A generates public/private key pair
2. Router A sends its public key to Router B
3. Router A encrypts packet with its private key and sends encrypted packet to Router B
4. Router B receives encrypted packet and decrypts with Router A's public key

Secret Key Encryption



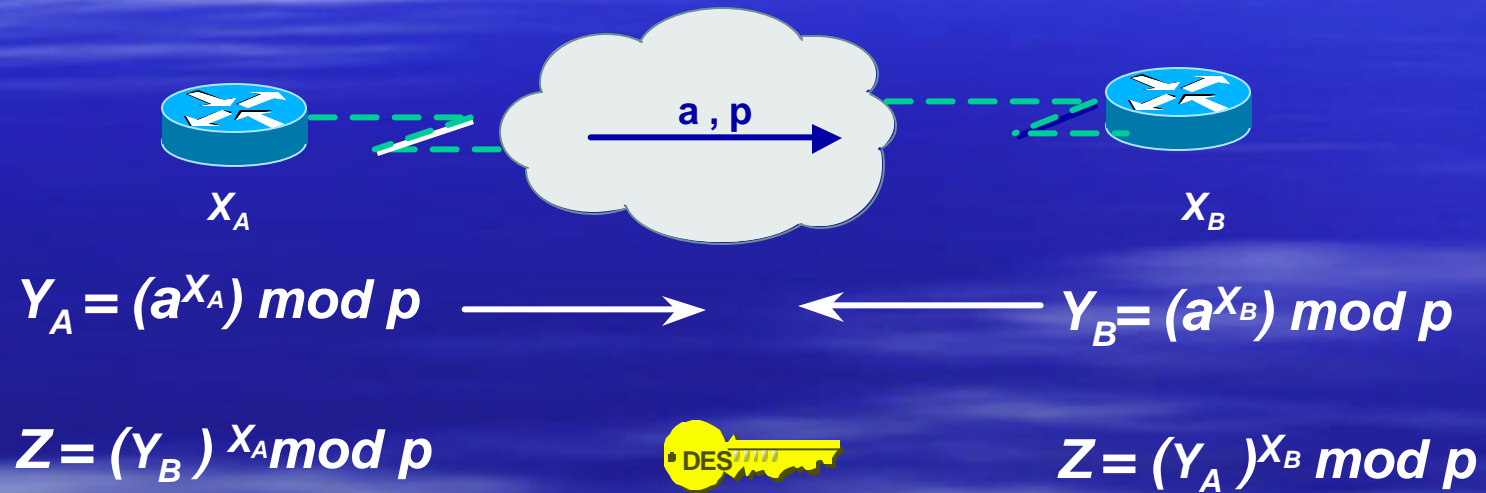
Common Algorithms: DES, 3DES, AES, IDEA

Scalability with Secret Key Crypto

Configuring shared secret keys easily
becomes administrative nightmare

Automated mechanism to securely derive
secret keys => Diffie-Hellman

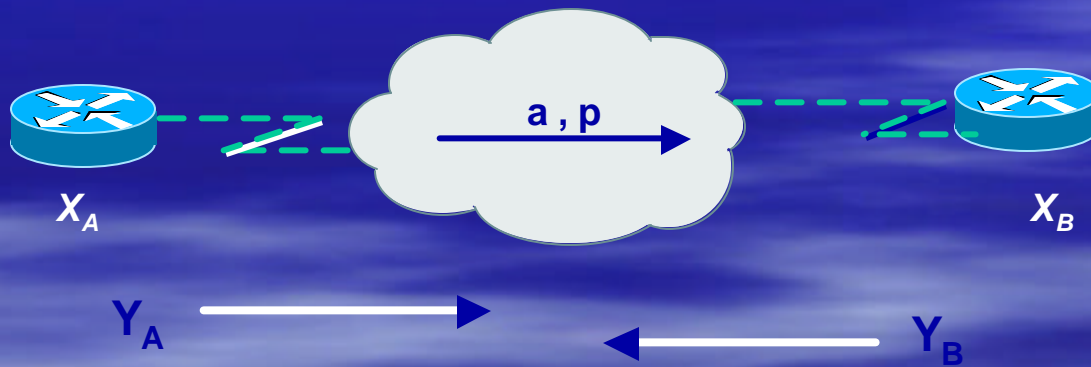
Deriving Secret Keys Using Public Key Technology (e.g., Diffie-Hellman)



By exchanging numbers in the clear,
two entities can determine a new unique
number (Z), known only to them

DH Man-in-the-Middle Attack

- Diffie-Hellman is subject to a man-in-the-middle attack
- Digital signatures of the 'public values' can enable each party to verify that the other party actually generated the value



=> DH exchanges need to be authenticated!!

Hash Functions

A *hash function* takes an input message of arbitrary length and outputs fixed-length code. The fixed-length output is called the *hash*, or the *message digest*, of the original input message.

Common Algorithms: MD-5 (128), SHA-1 (160)

Exclusive –OR Function (X-OR)

$$1 \text{ xor } 1 = 0$$

$$0 \text{ xor } 0 = 0$$

$$1 \text{ xor } 0 = 1$$

$$0 \text{ xor } 1 = 1$$

0 1 1 0 0 1 0 1 xor'ed with 1 1 0 1 0 0 1 1 produces 1 0 1 1 0 1 1 0

1 0 1 1 0 1 1 0 xor'ed with 1 1 0 1 0 0 1 1 produces 0 1 1 0 0 1 0 1

Computing a Keyed-MAC

- Message broken down into n blocks of 512-bits
- Shared secret key is xor'ed with specified array to produce K1
- Shared secret key is xor'ed a 2nd time with another specified array to produce K2

$$\text{Hash1} = (1^{\text{st}} \text{ block of message} + \text{K1})_{\text{MD5}}$$

$$\text{Hash2} = (\text{hash1} + \text{K2})_{\text{MD5}}$$

$$\text{Hash3} = (2^{\text{nd}} \text{ block of message} + \text{hash2})_{\text{MD5}}$$

$$\text{Hash}(n+1) = (n^{\text{th}} \text{ block of message} + \text{hash}_n)_{\text{MD5}}$$

HMAC-MD5-96 / HMAC-SHA-96 -> last hash truncated to 96 bits!!

Digital Signatures



- A digital signature is a message appended to a packet
- Used to prove the identity of the sender and the integrity of the packet

Digital Signatures

- Two common public-key digital signature techniques:
 - RSA (Rivest, Shamir, Adelman)
 - DSS (Digital Signature Standard)
- A sender uses its private key to **sign** a packet. The receiver of the packet uses the sender's public key to **verify** the signature.
- Successful verification assures:
 - The packet has not been altered
 - The identity of the sender

Crypto 101 Summary

- Public Key Encryption
 - Typically used for data origin authentication
 - Often combined with hash function
- Secret Key Encryption
 - Typically used for data confidentiality
- Diffie-Hellman Algorithm
 - Uses public-key cryptography to derive secret key
 - Exchanges need to be authenticated
- Hash Functions
 - Easy to compute
 - Typically used for data origin authentication and data integrity
- Digital Signatures
 - Combines hash functions with public key cryptography

Technology Fundamentals

- Crypto 101
- **Authentication Technologies**
- Application Layer Security
- Transport Layer Security
- Network Layer Security (IPsec)
- Link Layer Security

Methods of Authentication

WHO are you? What credentials do you give?

Weak

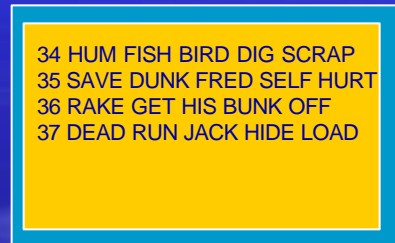
- No username/password
- Static username/password
- Aging username/password
- One-Time Password (OTP)
 - S/Key—OTP for terminal login
 - PAP—OTP for PPP
- Token cards/soft tokens (OTP)
 - Enigma Logic, DES Card, Security Dynamics

Strong

One Time Passwords

- S/KEY

- List of one-time passwords

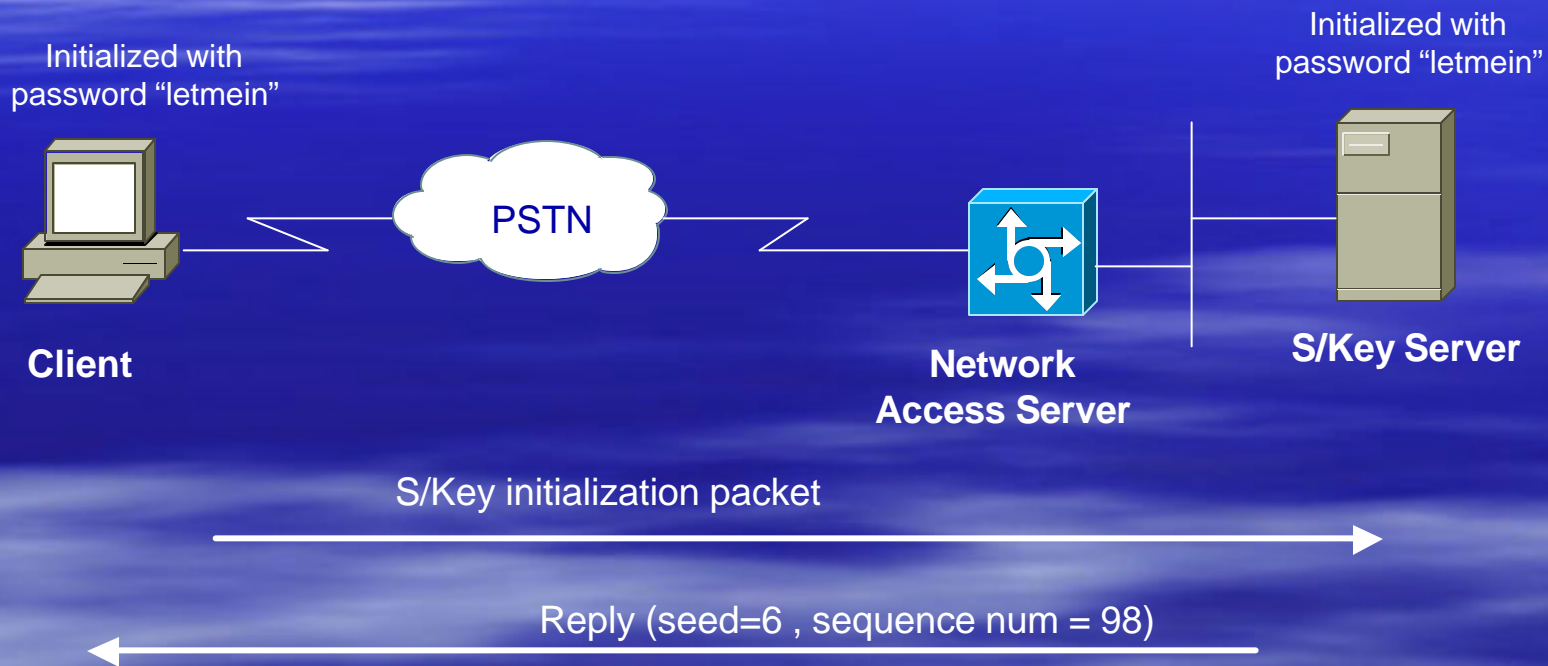


- Token cards

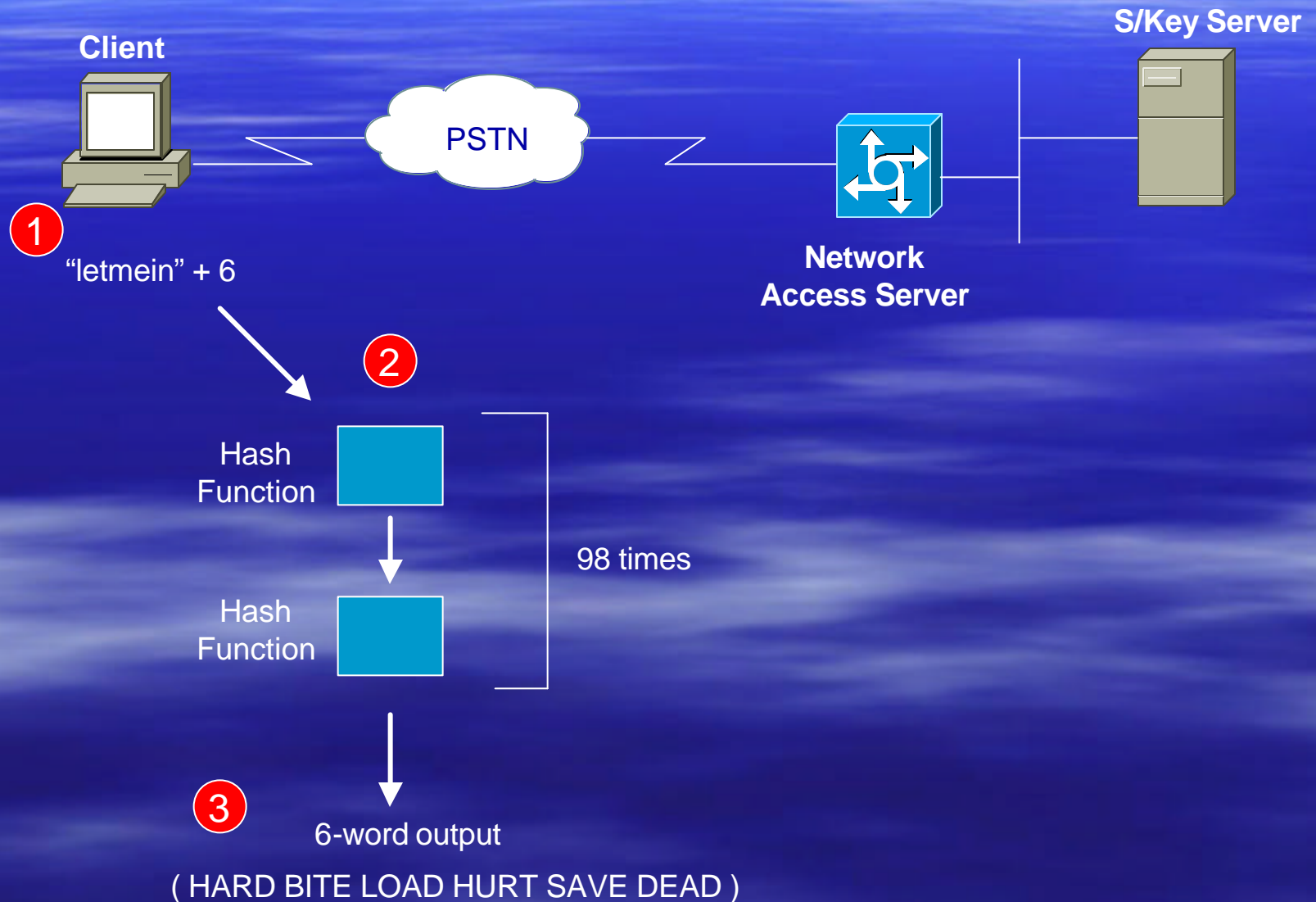
- Use algorithm based on PIN or time-of-day to generate passwords
 - Server uses same algorithm



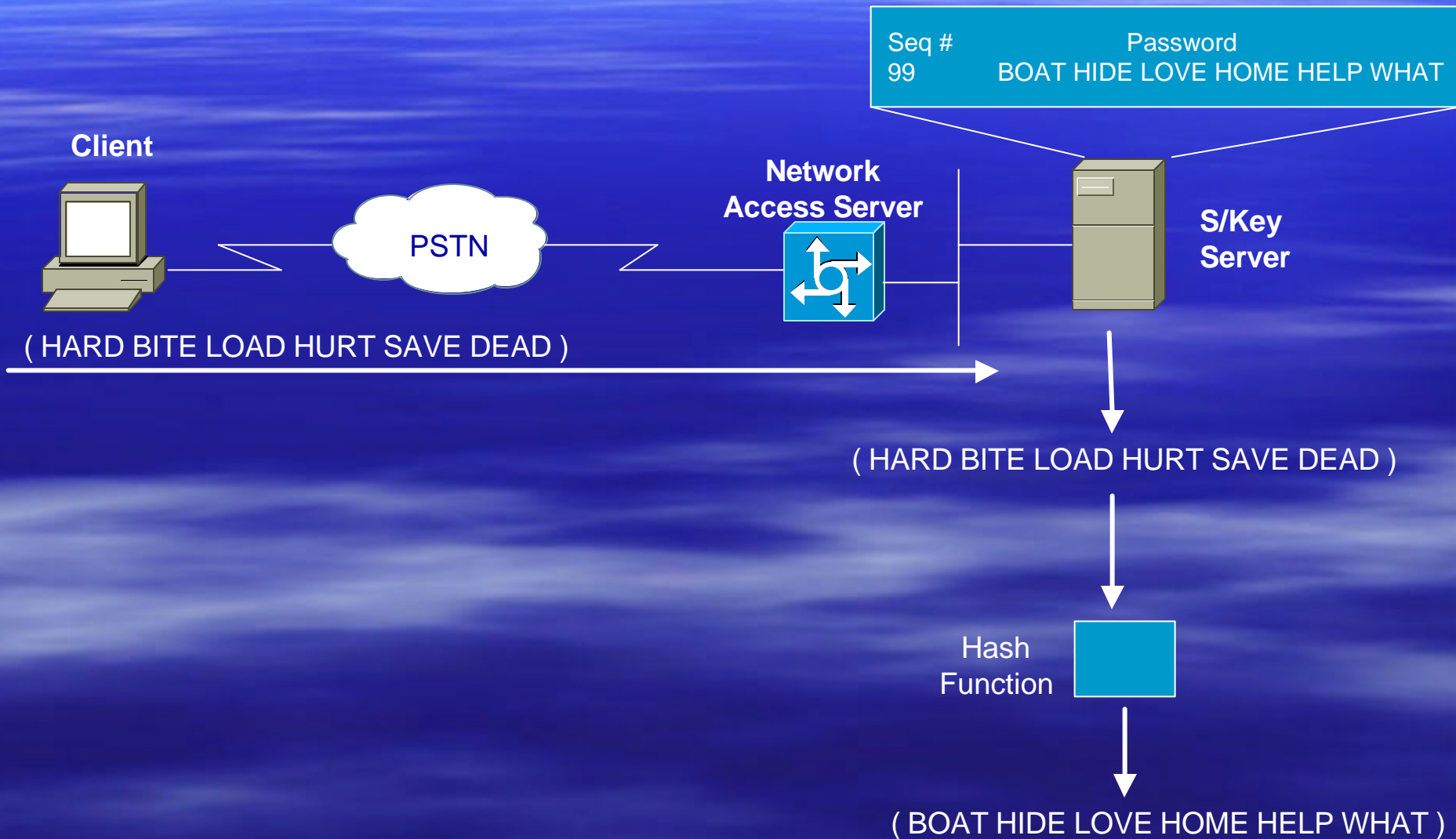
Initial S/Key Exchange



S/Key Password Computation



Verifying The S/Key Password



S/Key Resources

- Free UNIX implementations
- Microsoft ?

Why Is PPP Important?

- Multiplex multiple protocols over a single connection
- Handle compression and encryption at lowest possible layer
- Easy authentication at other end of connection
- You use it for dial-up connections

Do You Use PPPoE?

- Encapsulates PPP packets over Ethernet
- Simple bridge access device can provide subnet connection to remote access server
- Useful in ADSL environments to provide access control, billing and type of service per-user, rather than per-site, basis

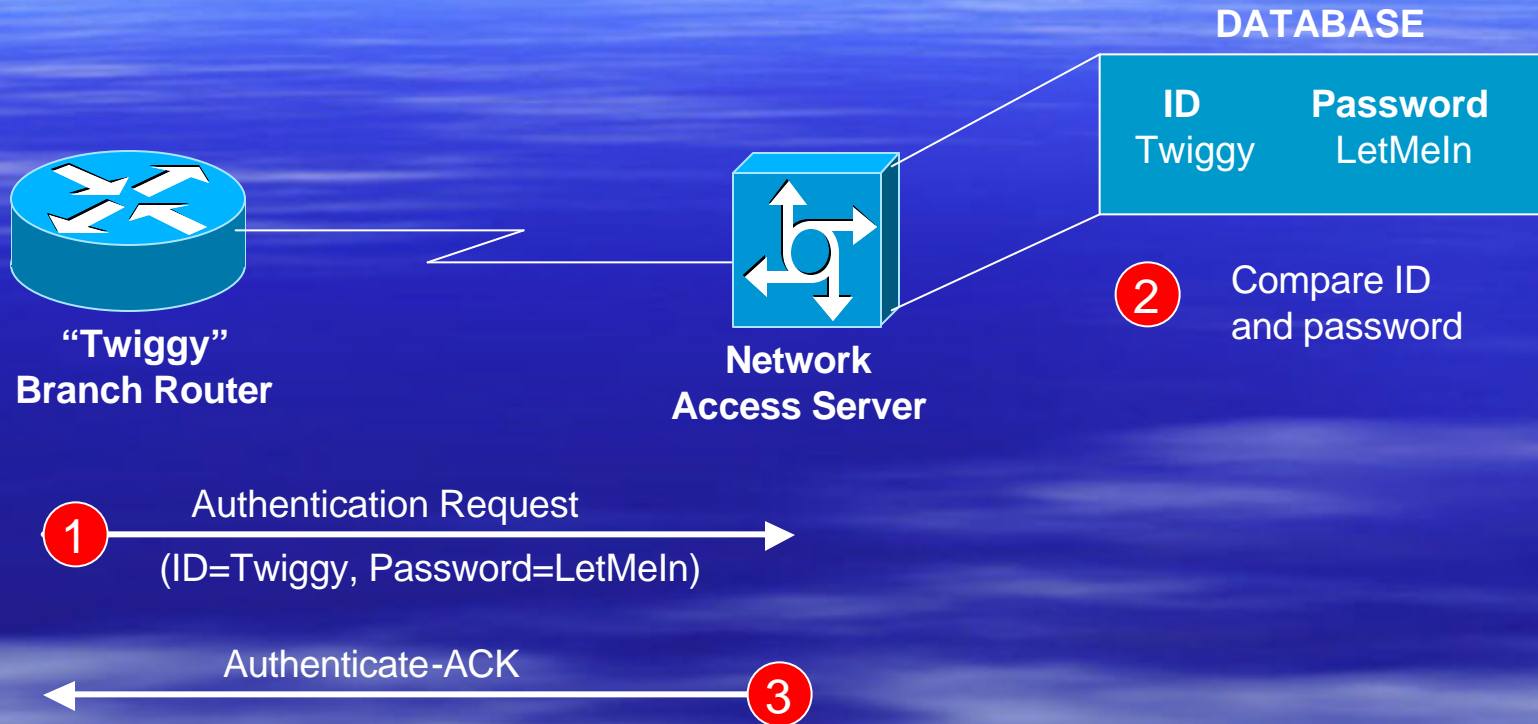
PPP Authentication

Link establishment (LCP) can be followed by optional authentication phase before proceeding to network layer protocol (NCP) phase.



- PAP
- CHAP
- MS-CHAP
- MS-CHAPv2
- EAP

PPP PAP Authentication

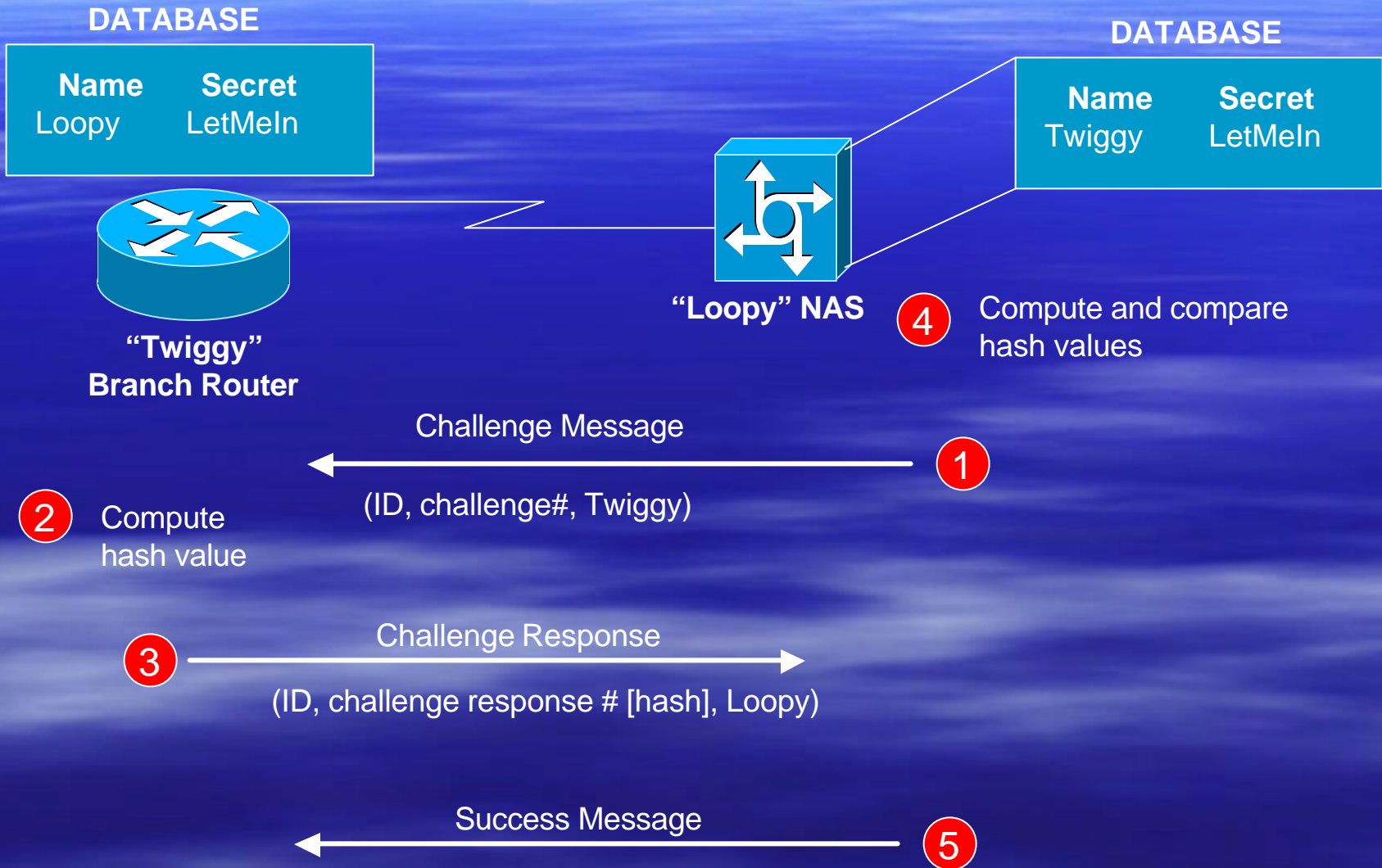


authenticates only client, authentication only performed once during session, passwords are sent in the clear

PPP CHAP Authentication

- Client and server need to exchange pre-shared secret
- Shared secret is used as input to hash function which computed 'challenge'
- Uses repeated challenges whose frequency is up to the authenticator to limit the time of exposure to any single attack
- Either CHAP peer can act as authenticator

PPP CHAP Authentication



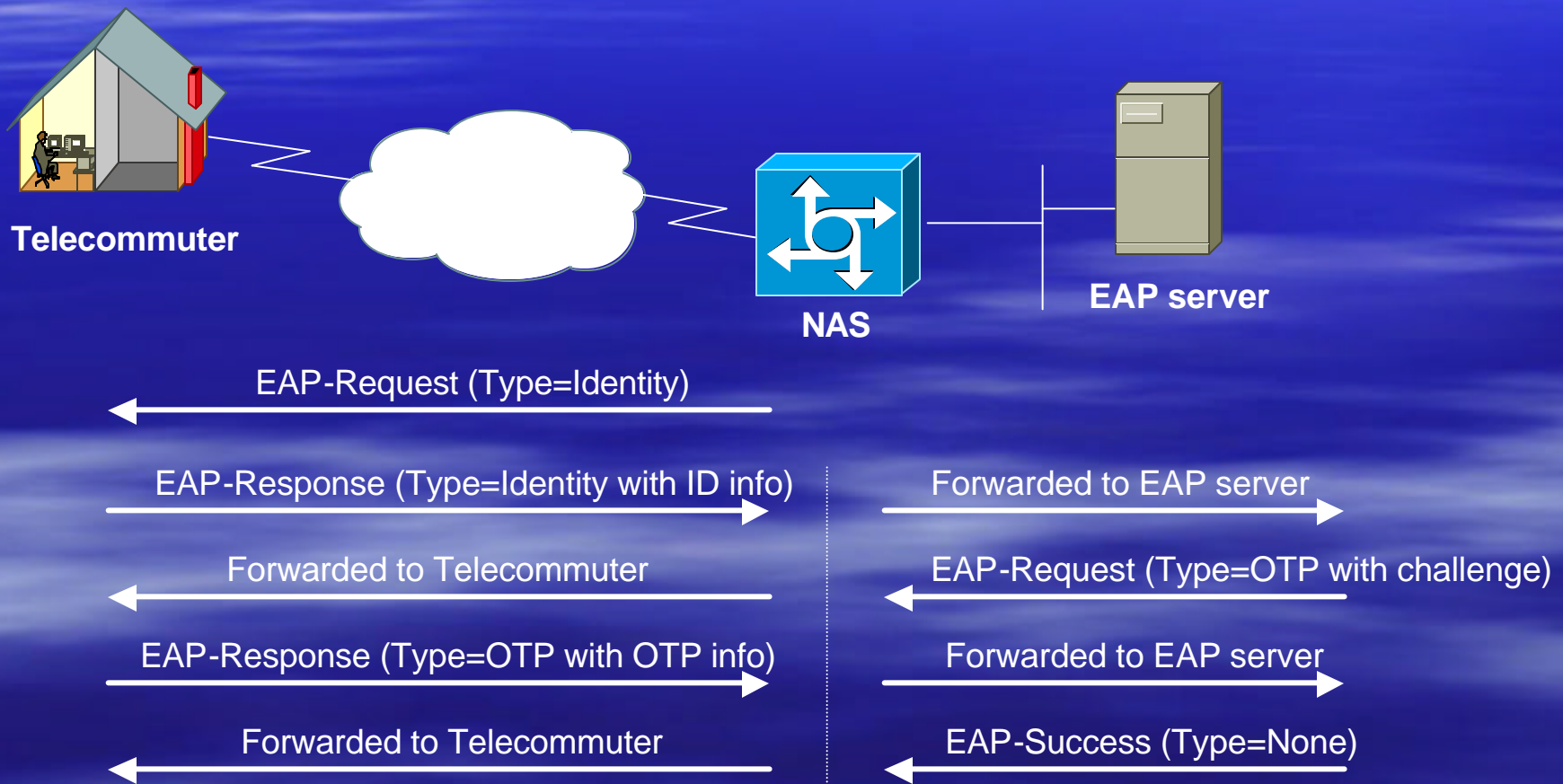
PPP MS-CHAP /MS-CHAP2

- RFC 1994 claims that CHAP secrets cannot be stored in encrypted form
- Microsoft has a variation of CHAP where the secrets are stored encrypted by both the peer and the authenticator

PPP EAP Authentication

- Supports multiple authentication mechanisms
- Authentication mechanism selected in authentication phase
- Permits use of a 'back-end' server
- NAS can become pass-through and doesn't need to be updated for new authentication mechanism support

PPP EAP Authentication



PPP Authentication Summary

- PPP PAP – password sent in clear; no playback protection....PAP should be avoided
- PPP CHAP – encrypted password but the password must be stored as cleartext on the server (not with MS-CHAP)
- PPP MS-CHAP - proprietary
- PPP EAP – most flexible

Scalable Authentication

- AAA: Provides for authentication as well as authorization and accounting
 - TACACS+
 - RADIUS
- Kerberos

TACACS+ Transactions

- Transactions between client and server are authenticated through use of shared secret
- Transactions are encrypted

- 1 Hash1 = (session ID, secret, version#, seq#) _{MD5}
Hash2 = (hash1, session ID, version#, seq#) _{MD5}
[repeated an implementation specific # of times]
- 2 Last hash concatenated and truncated to length of data to be encrypted....this is called the pseudo-pad
- 3 Ciphertext = bitwise XOR on pseudopad with data to be encrypted

TACACS+ Header

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Major	Minor	Type	Sequence Number	Flags
Session ID				
Length				

Major version: major TACAS+ version number

Minor version: minor TACACS+ version number which allows revisions
To the TACACS+ protocol while maintaining backwards compatibility

Type: 0x01=authentication; 0x02=authorization; 0x03=accounting

Seq_num: the first TACACS+ packet in a session must start with 1
And each subsequent packet increments the sequence number by 1

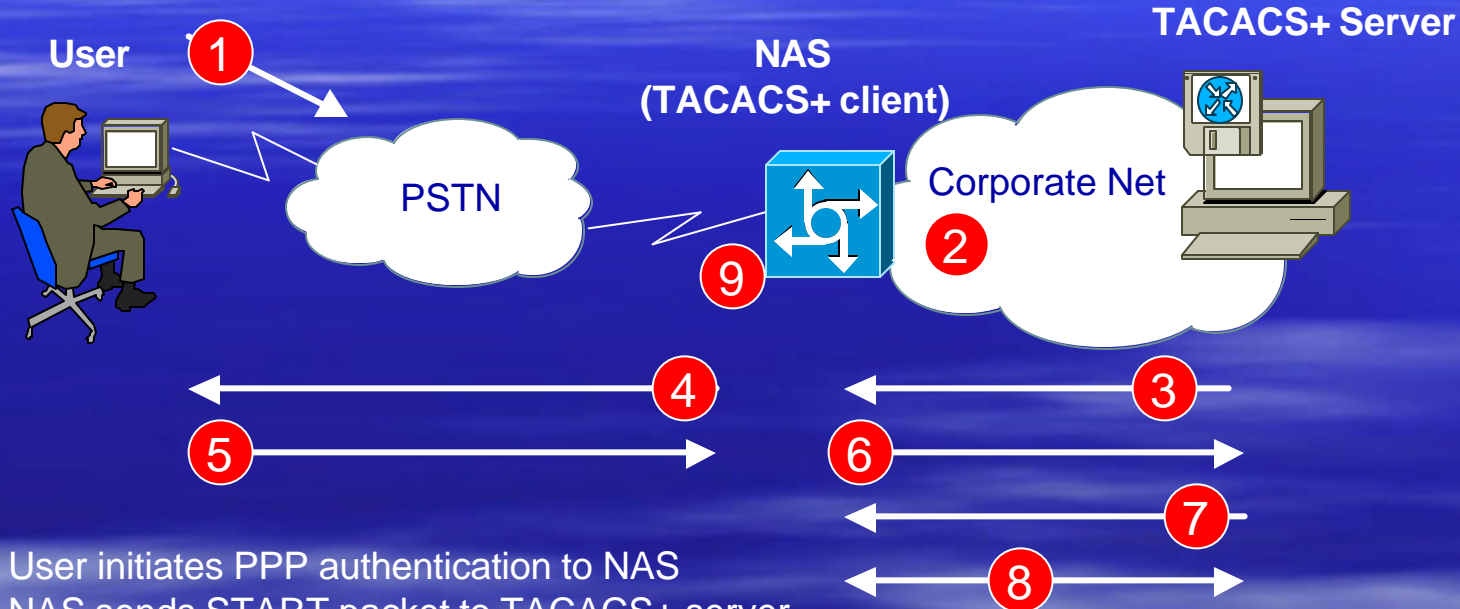
Flags: specifies whether encryption or multiplexing is used

Session ID: randomly chosen and does not change for the duration
Of the TACACS+ session

Length: total length of the TACACS+ packet excluding the header

A TACACS+ Exchange

TACACS+ client and server are pre-configured with a shared key



1. User initiates PPP authentication to NAS
2. NAS sends START packet to TACACS+ server
3. TACACS+ server responds with GETUSER packets that contain the prompts for username/password (PAP) or challenge (CHAP)
4. NAS sends the display to the user
5. User responds to NAS
6. NAS sends encrypted packet to TACACS+ server
7. TACACS+ server responds to NAS with authentication result
8. NAS and TACACS+ server exchange authorization requests and replies
9. NAS acts upon authorization exchange

RADIUS Transactions

- Transactions between client and server are authenticated using shared secret
 - Only user passwords are encrypted between client and server
- ① $\text{Hash1} = (\text{random\#, secret})_{\text{MD5}}$
 - ② User password is padded with nulls to get 16-bytes
 - ③ $\text{Encrypted Password} = \text{hash1 XOR padded password}$

RADIUS Packet Format

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Code	Identifier	Length
Request Authenticator		
Attributes		

Code: one octet and identifies the type of RADIUS packet


Identifier: one octet and aids in identifying requests and replies

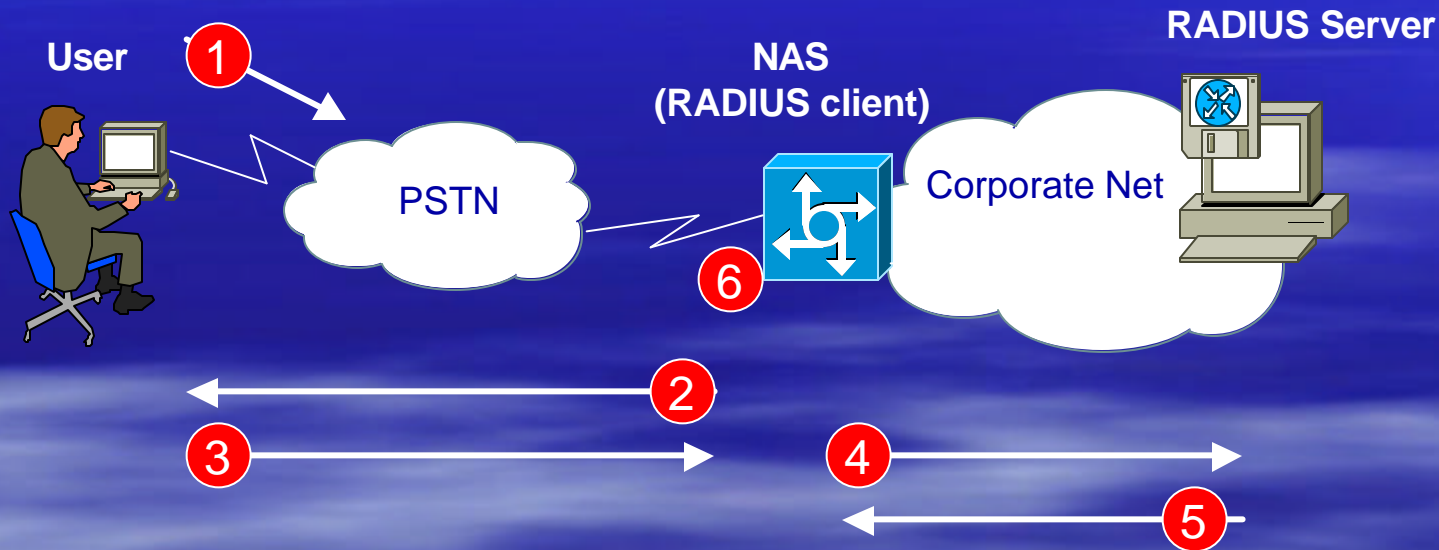
Length: two octets and indicates length of the packet including the Code, Identifier, Length, Authenticator and Attribute fields. The minimum Length is 20 and the maximum is 4096 octets.

Authenticator: 16 octets whose value is used to authenticate the reply From a RADIUS server and is used in the password encryption algorithm

Attributes: specifies what RADIUS services are used

RADIUS Login and Authentication

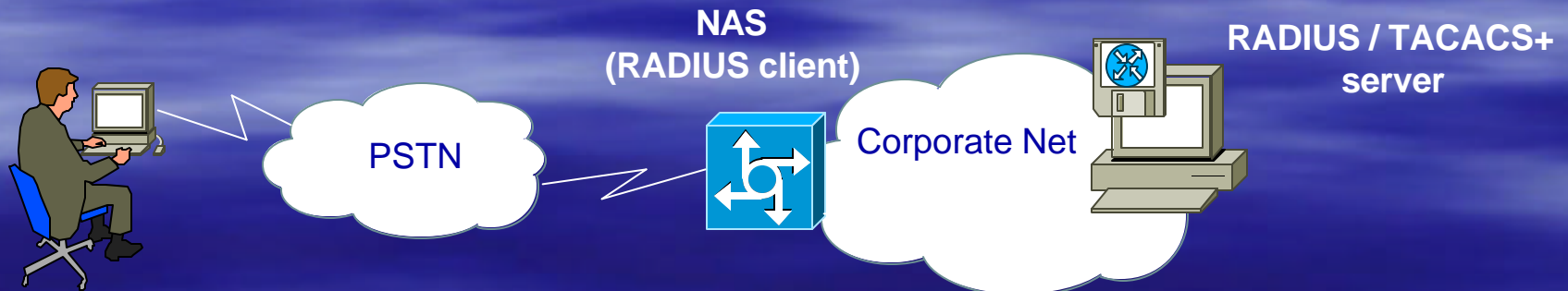
RADIUS client and server are pre-configured with a shared key 



1. User initiates PPP authentication to NAS
2. NAS prompts user for username/password (PAP) or challenge (CHAP)
3. User replies
4. NAS sends username and encrypted password to RADIUS server
5. RADIUS server responds with Accept, Reject or Challenge
6. NAS acts upon services and service parameters bundled with Accept or Reject

TACACS+ vs RADIUS

- TACACS+: TCP port 49
- RADIUS: UDP port 1812 (1645)
- Only password is confidential in RADIUS
- Feature support
- Vendor support

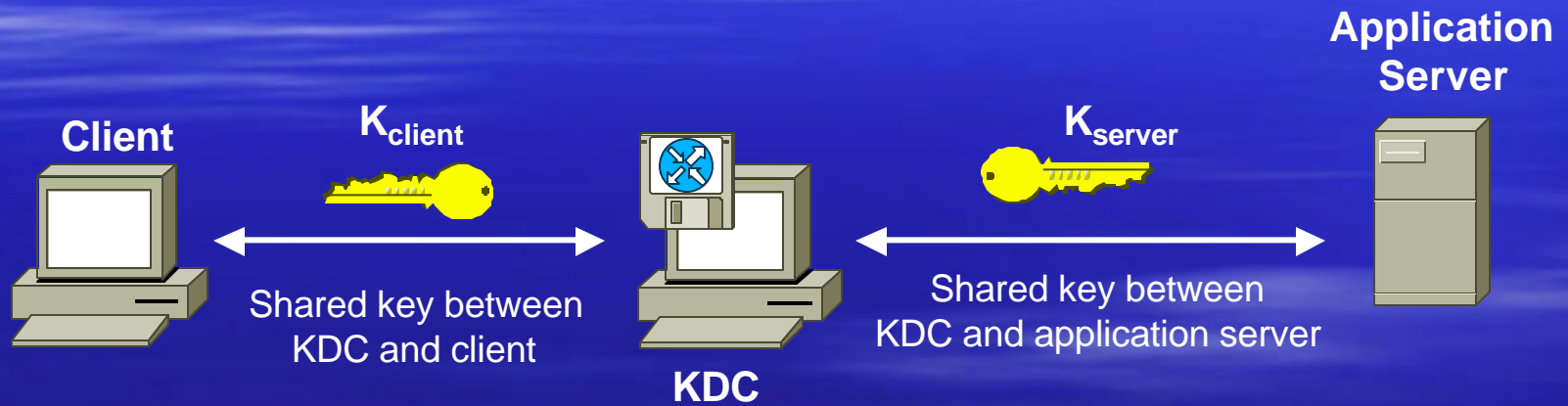


Where is info sent in cleartext?!?

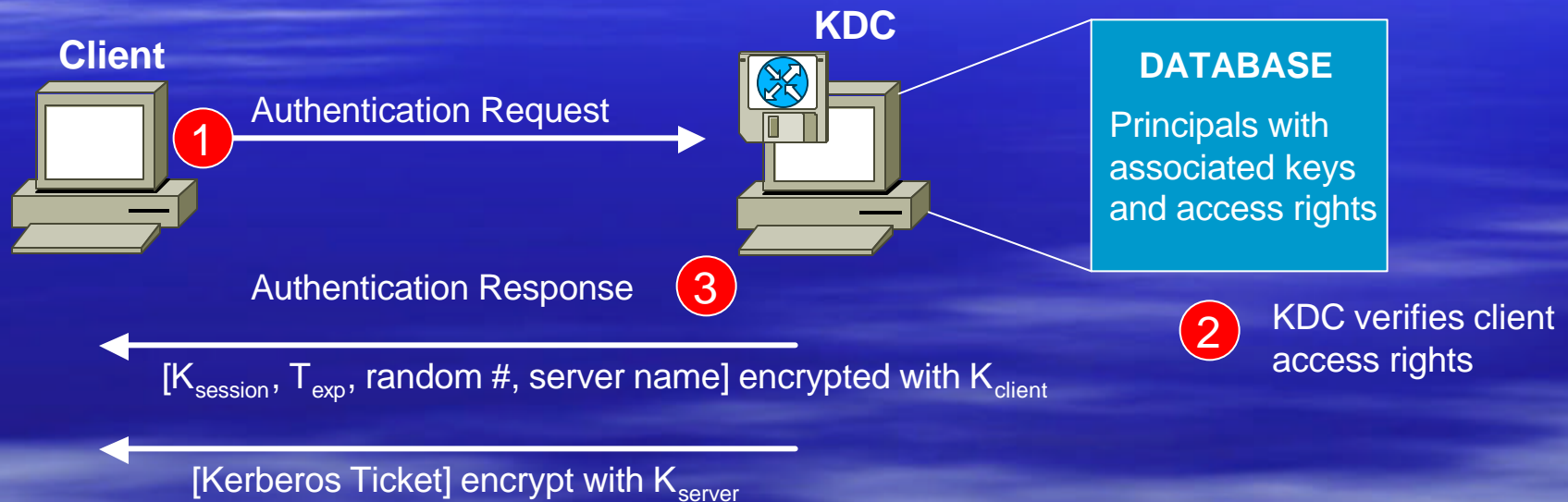
Keberos

- Designed at MIT
- Uses DES for encryption and authentication
- Uses a trusted third party (the KDC) to issue 'tickets' to users

Kerberos Keys

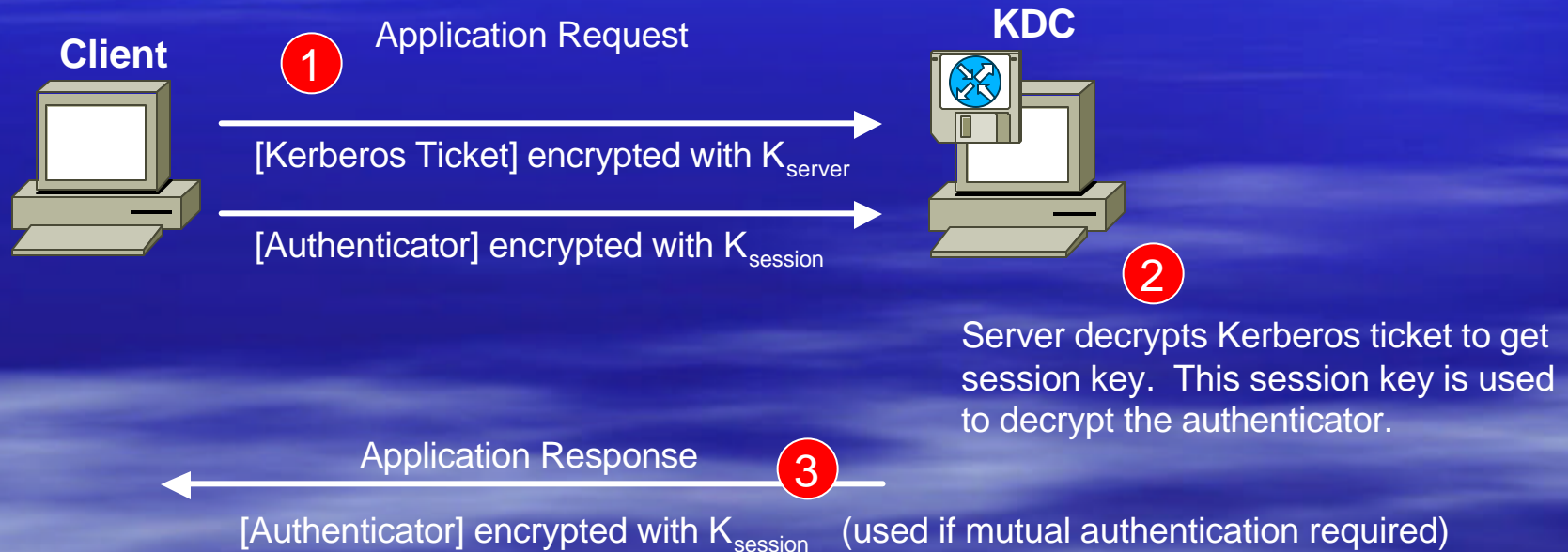


Kerberos Authentication Request and Reply



- 4** Client prompts user for password and uses the password, K_{client} to decrypt the session key K_{session}

Kerberos Application Request and Reply



Kerberos Timestamps

Since Kerberos has a time-dependency issue through use of timestamps, a synchronized dependable mechanism of obtaining time is needed.

Adding Access Control

Wouldn't it be cool if access to network points was denied unless successfully authenticated?

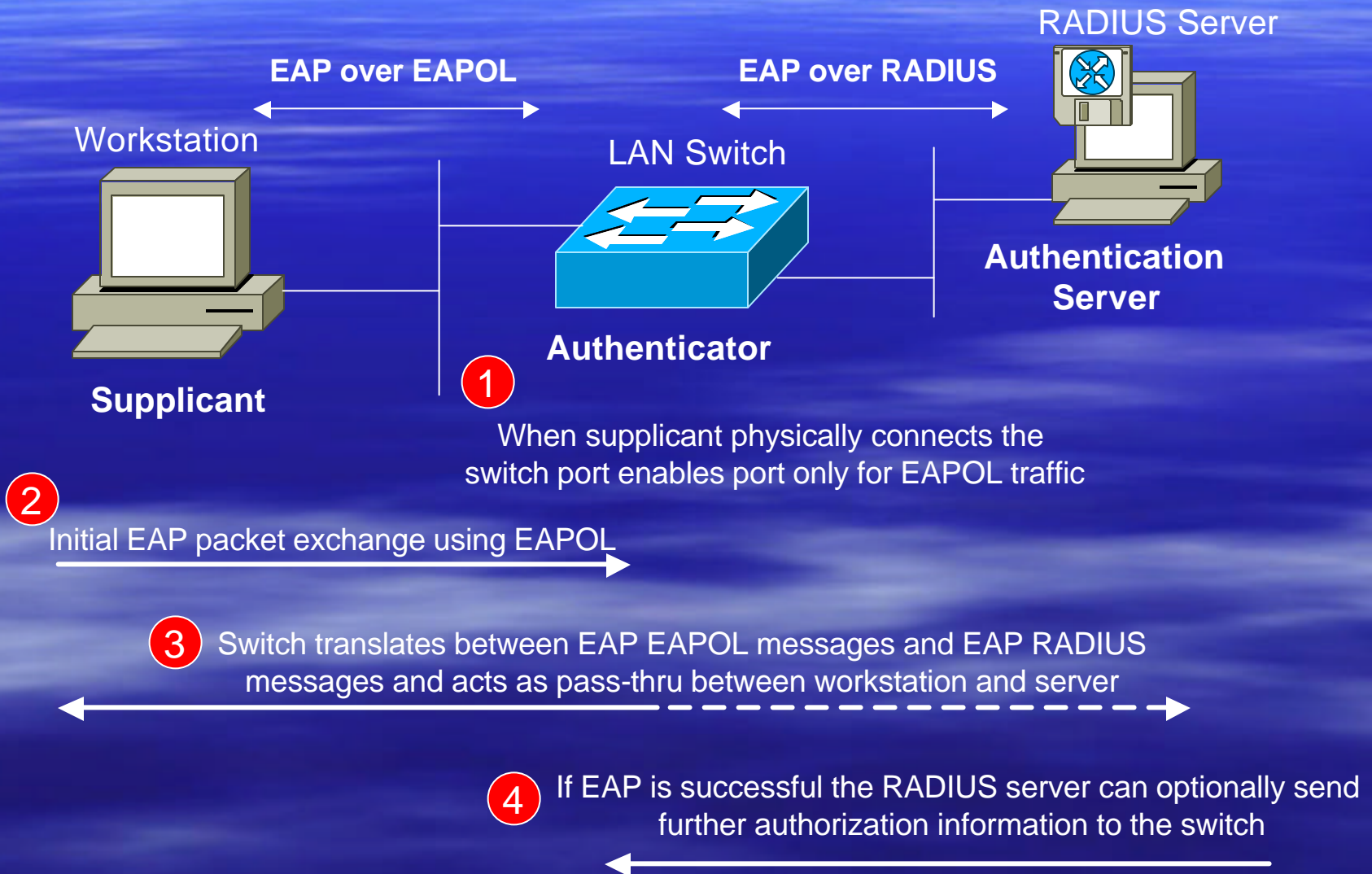
That's what 802.1x standard can be used for.....

IEEE 802.1x



- IEEE specification that enables authentication and key management for IEEE 802 local area networks
- Utilizes EAP for authentication

802.1x Transaction Example



Authentication Technology Summary

- Try to use one-time passwords wherever possible.
- PPP EAP with RADIUS is very flexible and scalable solution for dial-in environments.
- AAA solutions can be used in conjunction with most authentication functionality and give added benefit of authorization and accounting.
- 802.1x will replace proprietary port authentication features.

Technology Fundamentals

- Crypto 101
- Authentication Technologies
- **Application Layer Security**
- Transport Layer Security
- Network Layer Security (IPsec)
- Link Layer Security

Application Layer Security

- S-HTTP: allows request and reply messages to be signed, authenticated, encrypted, or any combination of these (including no protection).
- S/MIME: for email and messaging protocols

S/MIME Security Services

- Authentication
- Message integrity and nonrepudiation of origin (using digital signatures)
- Privacy and data security (using symmetric encryption)

It is up to implementation to decide whether to sign or encrypt first !!

Technology Fundamentals

- Crypto 101
- Authentication Technologies
- Application Layer Security
- **Transport Layer Security**
- Network Layer Security (IPsec)
- Link Layer Security

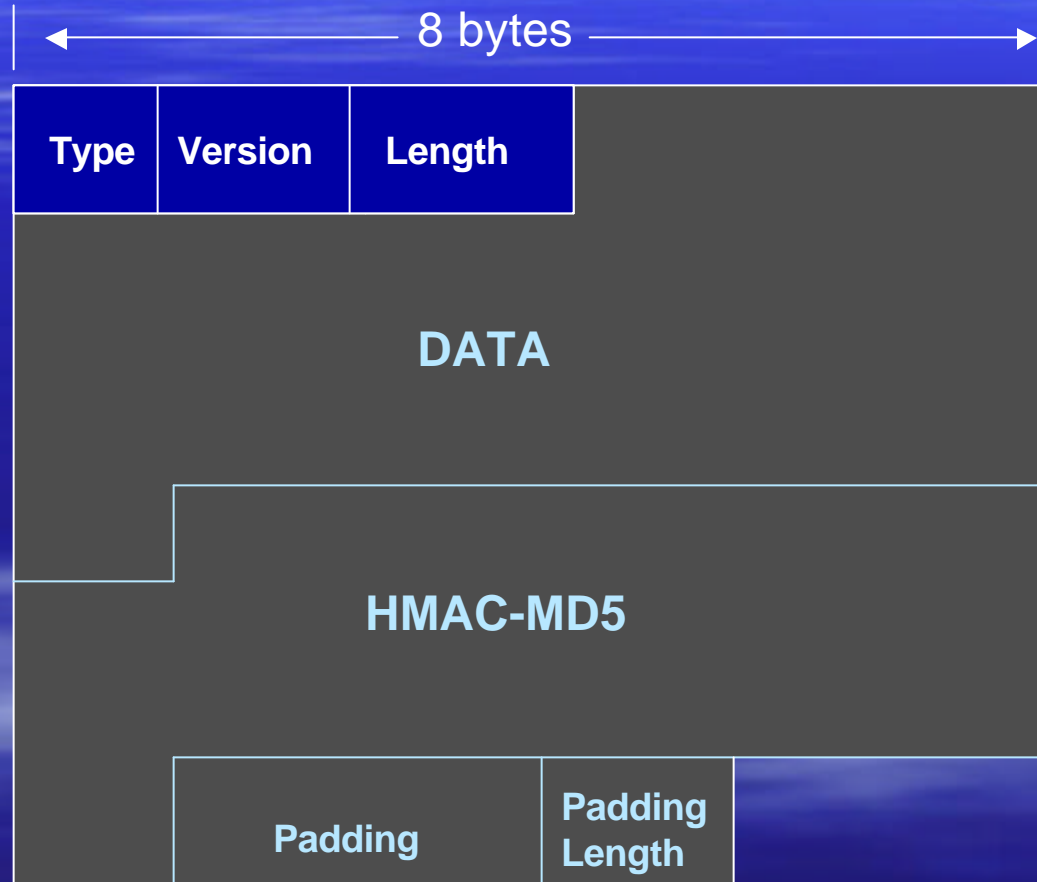
Transport Layer Security (SSL/TLS)

Provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.

3 Main Properties:

- The connection is private. Encryption is used after an initial handshake to define a secret key. Symmetric cryptography is used for data encryption (for example, DES and RC4).
- The peer's identity can be authenticated using asymmetric, or public key, cryptography (for example, RSA and DSS).
- The connection is reliable. Message transport includes a message integrity check using a keyed MAC. Secure hash functions (such as SHA and MD5) are used for MAC computations.

SSL/TLS Record Format



The SSL Handshake Process



1 Client initiates SSL connection / sends supported cipher suites

2 Server returns digital certificate to client and selected cipher suite

3 Client sends encrypted shared secret

4 Message encryption and integrity algorithms are negotiated

5 Session keys are generated

6 Secure session tunnel is established

SSL Client Authentication

- Client authentication (certificate based) is optional and not often used
- Many application protocols incorporate their own client authentication mechanism such as username/password or S/Key
- These authentication mechanisms are more secure when run over SSL

SSL/TLS IANA Assigned Port Numbers

Protocol	Defined Port Number	SSL/TLS Port Number
HTTP	80	443
NNTP	119	563
SMTP	110	995
FTP-Data	20	989
FTP-Control	21	990
Telnet	23	992

Secure Shell (SSH)

- Secure low-level transport protocol
- Provides strong encryption, cryptographic host authentication, and integrity protection
- Authentication is host-based and does not perform user authentication
- A higher-level protocol for user authentication can be designed on top of SSH.
- The key exchange method, the public key algorithm, the symmetric encryption algorithm, the message authentication algorithm, and the hash algorithm are all negotiated.
- Widely supported across multiple operating systems.

Technology Fundamentals

- Crypto 101
- Authentication Technologies
- Application Layer Security
- Transport Layer Security
- Network Layer Security (IPsec)
- Link Layer Security

IPsec

Suite of protocols to secure IP traffic

- Defined in RFC 2401-2409, RFC 2451
- ietf.org/html.charters/ipsec-charter.html

What Does IPsec Provide?

- Confidentiality....many algorithms to choose from
- Data integrity and source authentication
 - Data “signed” by sender and “signature” verified by the recipient
 - Modification of data can be detected by signature “verification”
 - Because “signature” based on a shared secret, it gives source authentication

What Does IPsec Provide?

- Anti-replay protection
 - Optional : the sender must provide it but the recipient may ignore
- Key Management
 - IKE – session negotiation and establishment
 - Sessions are rekeyed or deleted automatically
 - Secret keys are securely established and authenticated
 - Remote peer is authenticated through varying options

What is an SA?

- Security Association groups elements of a conversation together
 - AH authentication algorithm and keys
 - ESP encryption algorithm and key(s)
 - Cryptographic synchronization
 - SA lifetime
 - SA source address
 - Mode (transport or tunnel)

A Security Association Maps:

- From a host or gateway
 - To a particular IP destination address
 - With a particular security protocol (AH/ESP)
 - Using SPI selected by remote host or gateway
- To a host or gateway
 - To (one of) our IP address(es)
 - With a particular security protocol (ESP/AH)
 - Using SPI selected by us

A SPI Represents an SA

- The SPI is a 32-bit number
- The SPI is combined with the protocol (AH/ESP) and destination IP address to uniquely identify an SA
- An SA is unidirectional

When an ESP/AH packet is received, the SPI is used to look up all of the crypto parameters

IPsec Traffic Selectors

- Selectors for traffic matches....what kind of traffic will be acted on how
- Selectors include:
 - IP address or range
 - Optional IP protocol (UDP, TCP, etc)
 - Optional layer 4 (UDP, TCP) port
- Selected traffic is either protected with IPsec or dropped

IPsec Components

- AH
 - RFC requires HMAC-MD5-96 and HMAC-SHA1-96....older implementations also support keyed MD5
- ESP
 - RFC requires DES 56-bit CBC and Triple DES. Can also use RC5, IDEA, Blowfish, CAST, RC4, NULL
- IKE

Authentication Header (AH)

- Authentication is applied to the entire packet, with the mutable fields in the IP header zeroed out
- If both ESP and AH are applied to a packet, AH follows ESP

AH Header Format

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Next Header	Payload Length	Reserved
Security Parameter Index (SPI)		
Sequence Number		
Authentication Data [Integrity Value Check (ICV)]		

Next Header: which higher level protocol is (UDP,TCP,ESP) next

Payload Length: size of AH in 32-bit longwords, minus 2

Reserved: must be zero

SPI: arbitrary 32-bit number that specifies to the receiving device which security association is being used (security protocols, algorithms, keys, times, addresses, etc)

Sequence Number: start at 1 and must never repeat. It is always set but receiver may choose to ignore this field

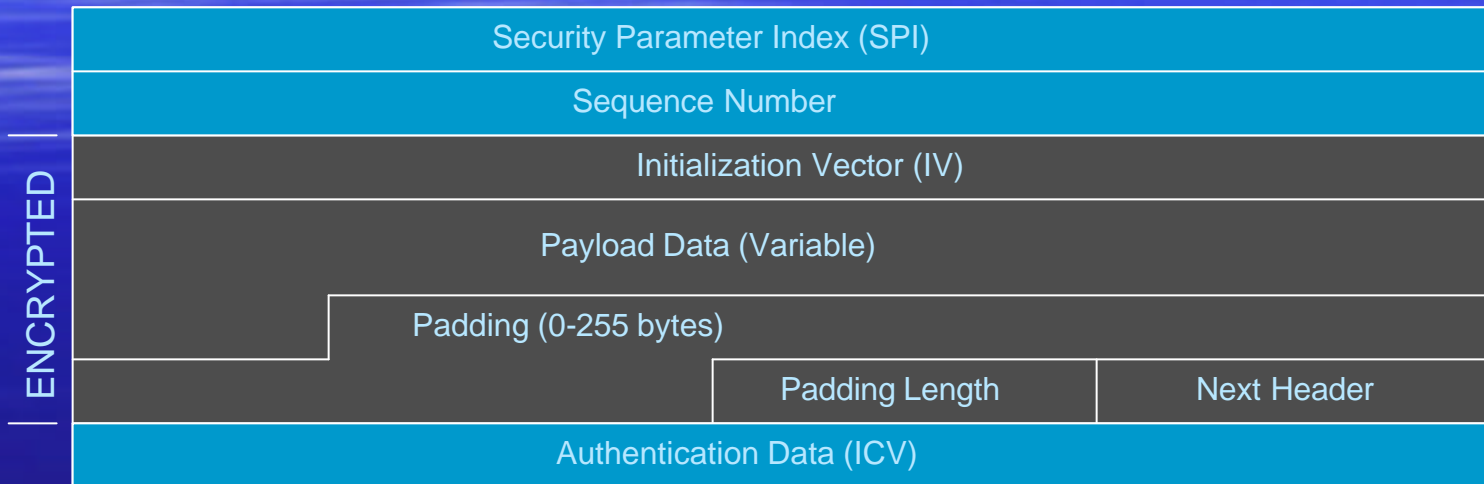
Authentication Data: ICV is a digital signature over the packet and it varies in length depending on the algorithm used (SHA-1, MD5)

Encapsulating Security Payload (ESP)

- Must encrypt and/or authenticate in each packet
- Encryption occurs before authentication
- Authentication is applied to data in the IPsec header as well as the data contained as payload

ESP Header Format

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31



SPI: arbitrary 32-bit number that specifies SA to the receiving device

Seq #: start at 1 and must never repeat; receiver may choose to ignore

IV: used to initialize CBC mode of an encryption algorithm

Payload Data: encrypted IP header, TCP or UDP header and data

Padding: used for encryption algorithms which operate in CBC mode

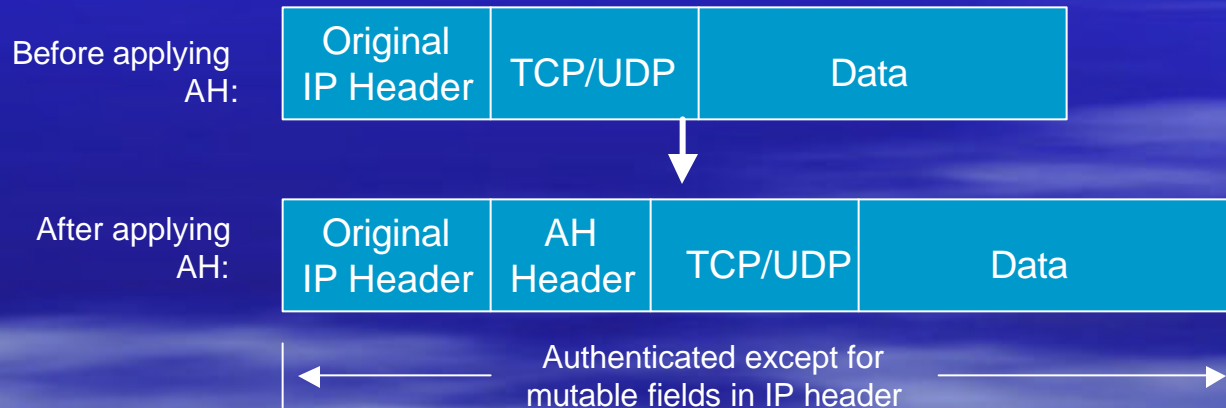
Padding Length: number of bytes added to the data stream (may be 0)

Next Header: the type of protocol from the original header which appears in the encrypted part of the packet

Authentication Header: ICV is a digital signature over the packet and it varies in length depending on the algorithm used (SHA-1, MD5)

Packet Format Alteration for AH Transport Mode

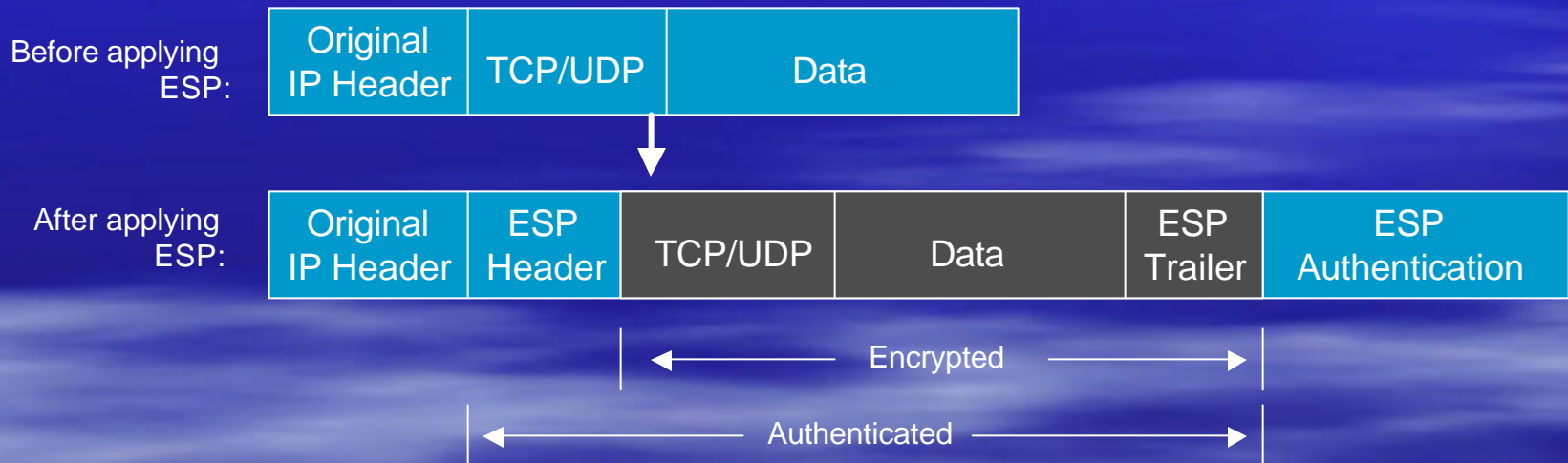
Authentication Header



- ToS
- TTL
- Header Checksum
- Offset
- Flags

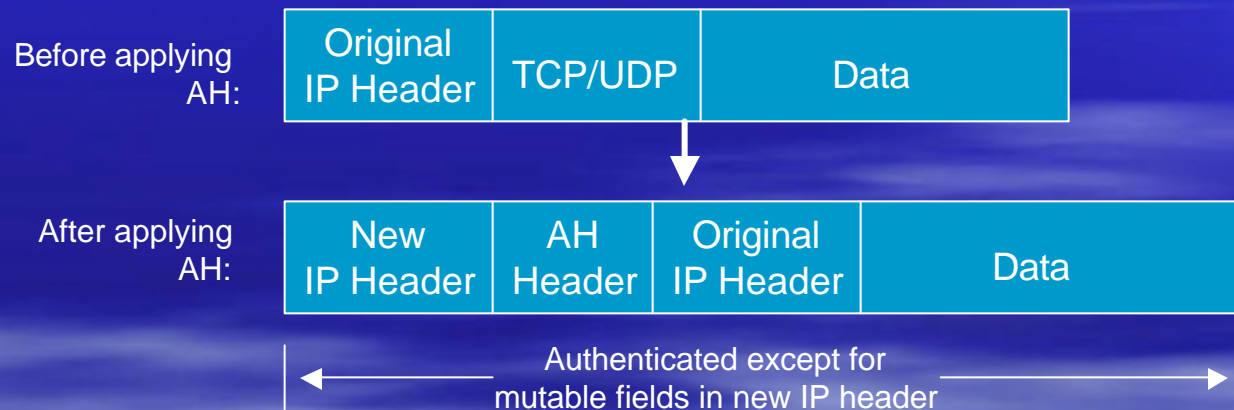
Packet Format Alteration for ESP Transport Mode

Encapsulating Security Payload



Packet Format Alteration for AH Tunnel Mode

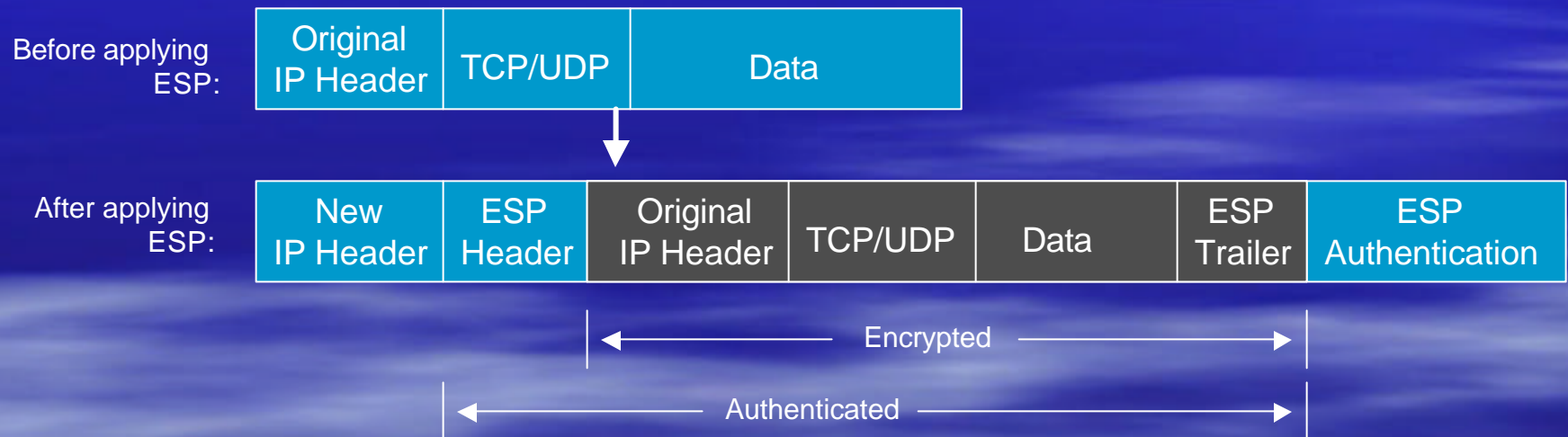
Authentication Header



- ToS
- TTL
- Header Checksum
- Offset
- Flags

Packet Format Alteration for ESP Tunnel Mode

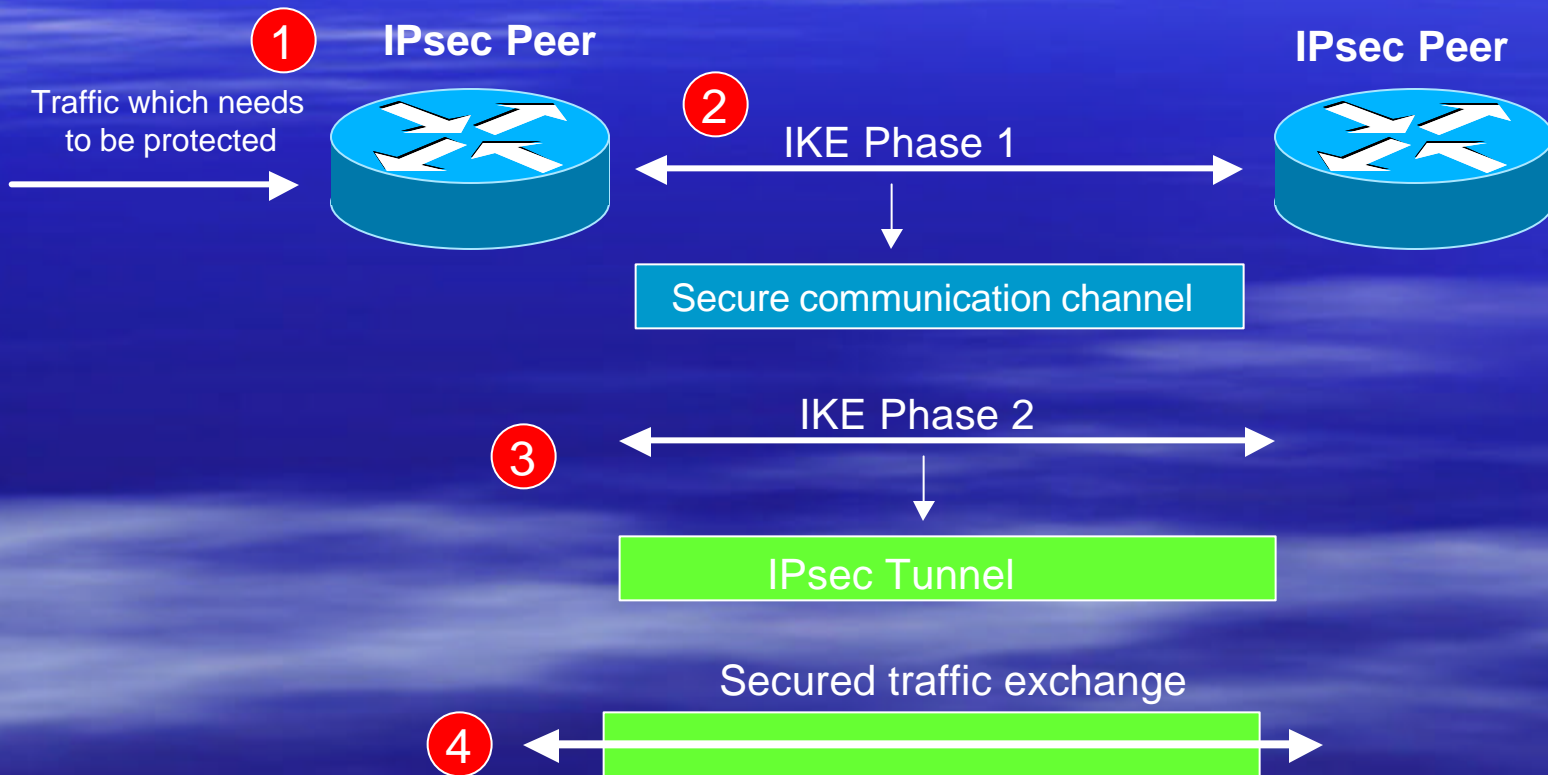
Encapsulating Security Payload



Internet Key Exchange (IKE)

- Phase I
 - Establish a secure channel (ISAKMP/IKE SA)
 - Using either main mode or aggressive mode
- Phase II
 - Establishes a secure channel between computers intended for the transmission of data (IPsec SA)
 - Using quick mode

Overview of IKE



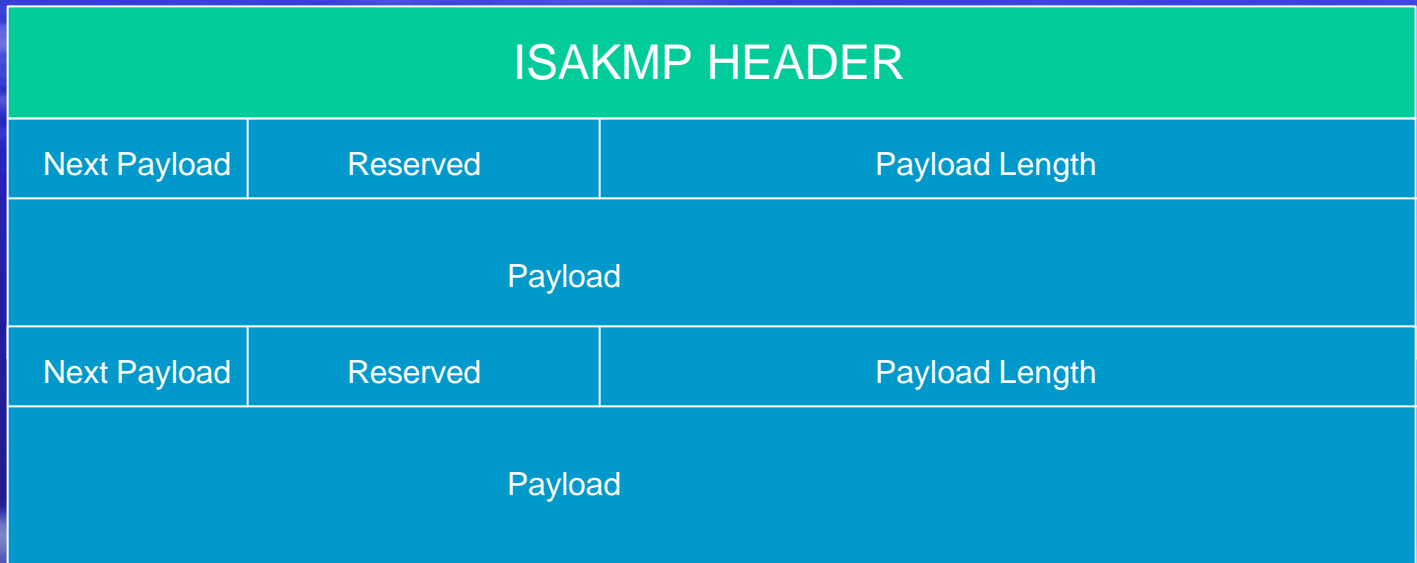
ISAKMP Header Format

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Initiator Cookie																															
Responder Cookie																															
Next Payload				Major Version				Minor Version				Exchange Type												Flags							
Message ID																															
Total Length of Message																															

ISAKMP Message Format

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31



Next Payload: 1 byte; identifier for next payload in message. If it is the last payload it will be set to 0

Reserved: 1 byte; set to 0

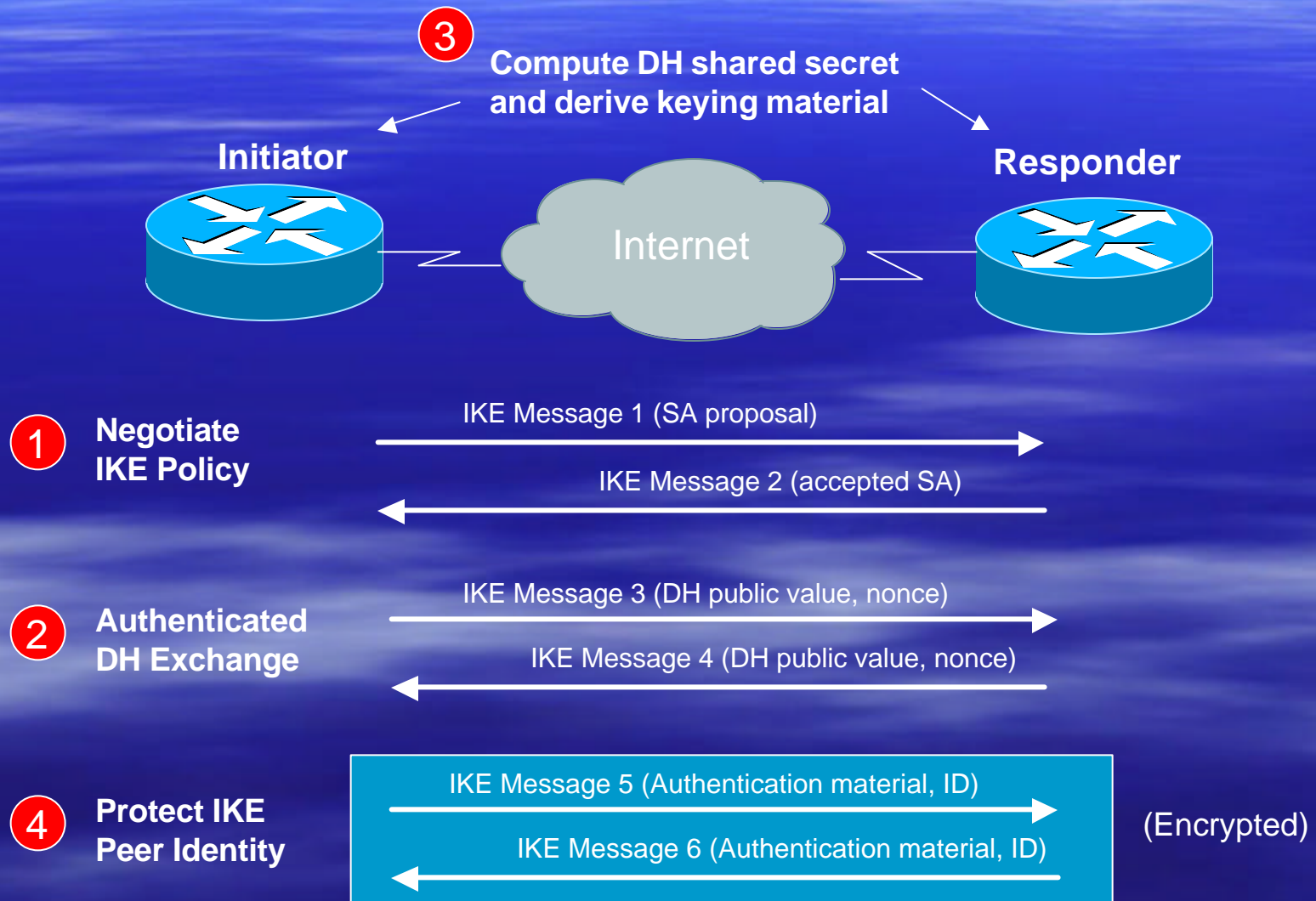
Payload Length: 2 bytes; length of payload (in bytes) including the header

Payload: The actual payload data

IKE Phase 1 Main Mode

- Main mode negotiates an ISAKMP SA which will be used to create IPsec SAs
- Three steps
 - SA negotiation (encryption algorithm, hash algorithm, authentication method, which DF group to use)
 - Do a Diffie-Hellman exchange
 - Provide authentication information
 - Authenticate the peer

IKE Phase 1 Main Mode



What Is Diffie-Hellman?

- First public key algorithm (1976)
- Diffie Hellman is a key establishment algorithm
 - Two parties in a DF exchange can generate a shared secret
 - There can even be N-party DF changes where N peers can all establish the same secret key
- Diffie Hellman can be done over an insecure channel
- IKE authenticates a Diffie-Hellman exchange 3 different ways
 - Pre-shared secret
 - Nonce (RSA signature)
 - Digital signature

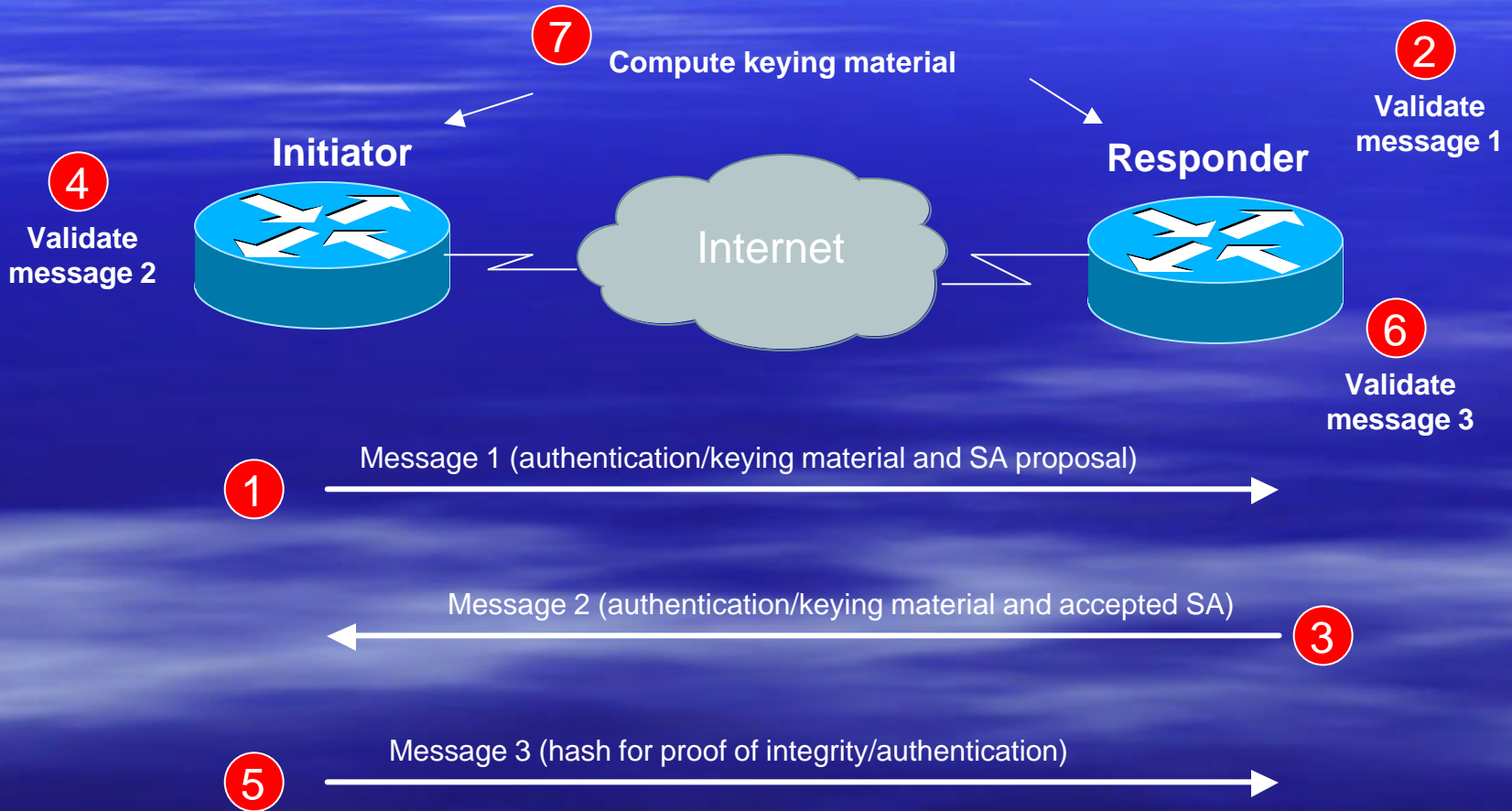
IKE Phase 1 Aggressive Mode

- Uses 3 (vs 6) messages to establish IKE SA
- No denial of service protection
- Does not have identity protection
- Optional exchange and not widely implemented

IKE Phase 2 Quick Mode

- All traffic is encrypted using the ISAKMP/IKE Security Association
- Each quick mode negotiation results in two IPsec Security Associations (one inbound, one outbound)
- Creates/refreshes keys

IKE Phase 2 Quick Mode



IKE Summary

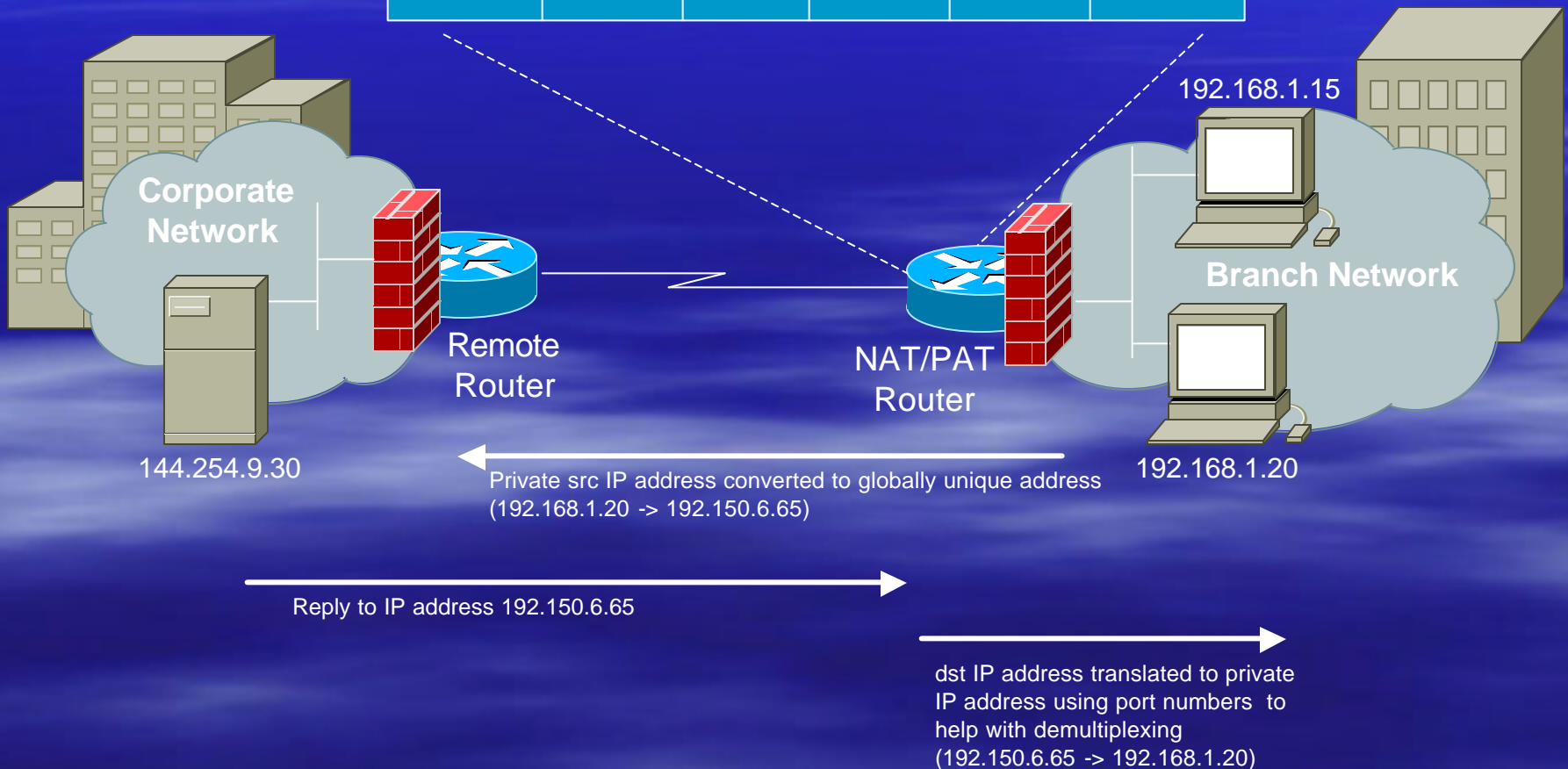
- Negotiates parameters to establish and secure a channel between two peers
- Provides mutual authentication
- Establishes authenticated keys between peers
- Manages IPsec SAs
- Provides options for negotiation and SA establishment
- LOOK FOR IKE v2 !!!

IPsec Issues

- Dynamic Addressing
- NAT/PAT
- Device vs User Authentication

NAT/PAT Problems

Original SRC IP	Translated SRC IP	Original SRC Port	Translated SRC Port	Original DST IP	Original DST Port
192.168.1.20	192.150.6.65	2654	6789	144.254.9.30	80
192.168.1.15	192.150.6.65	5876	6788	144.254.9.30	80

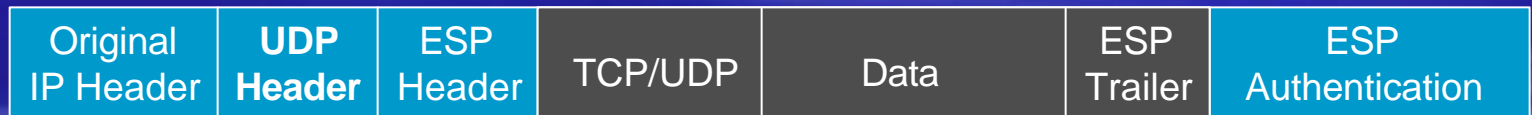


UDP Encapsulation of Transport Mode ESP Packets

Transport Mode



After applying ESP/UDP:

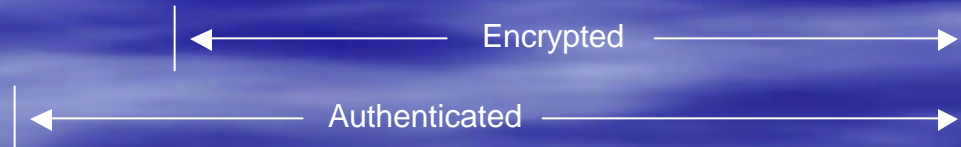


UDP Encapsulation of Tunnel Mode ESP Packets

Tunnel Mode



After applying ESP/UDP:



Technology Fundamentals

- Crypto 101
- Authentication Technologies
- Application Layer Security
- Transport Layer Security
- Network Layer Security (IPsec)
- **Link Layer Security**

Dial-Up VPNs

- Treat remote dial access as virtual (Point-to-point) links
 - Primary goal of L2 VPNs is tunneling, not security
 - Traditional dial-up user authentication (PAP, CHAP, MS-CHAP, EAP)
 - In some cases, data confidentiality

Layer 2 Tunneling Protocol

- Designed in IETF PPP Extensions working group
 - Combination of Cisco L2F & PPTP features, L2TP RFC 2661, Aug 99
 - L2TP Extensions working group established
- Uses UDP for control and data packets, well known port is 1701
- Uses PPP for packet encapsulation – carries most protocols (also non-IP protocols)
- IP UDP packet security provided by IPsec transport mode, as in RFC 2401, 2409, etc

L2TP Features

- Control session authentication, keep-alives
- EAP...broader authentication mechanisms
- Tunnel over any switched virtual connection (IP, FR, ATM)....runs over any transport
- Integration with mobile IP
- IPsec ESP for confidentiality and integrity (else packets in the 'clear')
- IKE for key management

L2TP and IPsec

Multiple Encapsulations
.....careful of packet size!!

IPsec DES or 3DES encrypted



Ping with large MTU size....help discover fragmentation issues!!

MPLS VPNs

Any VPN is **not** automagically secure.
You need to add security functionality to create secure VPNs. That means using firewalls for access control and probably IPsec for confidentiality and data origin authentication.

Agenda

- Session I (1:30 – 3:00)
Security Technology Details
- Session II (3:30 – 5:00)
Secure Infrastructure Architectures
- Session III (7:30 – 9:00)
Sample Configuration Scenarios

Security.....

Not Just a Technology Problem

- Vast quantities of security technologies
- The challenge — enable you as an ISP to implement a single policy
- **Get vendors to simplify configurations (what are reasonable defaults?!?)**
- Need to identify threats and vulnerabilities

Definitions

Threat: any person, object, or event that, if realized, can potentially cause damage to the network or networked device.

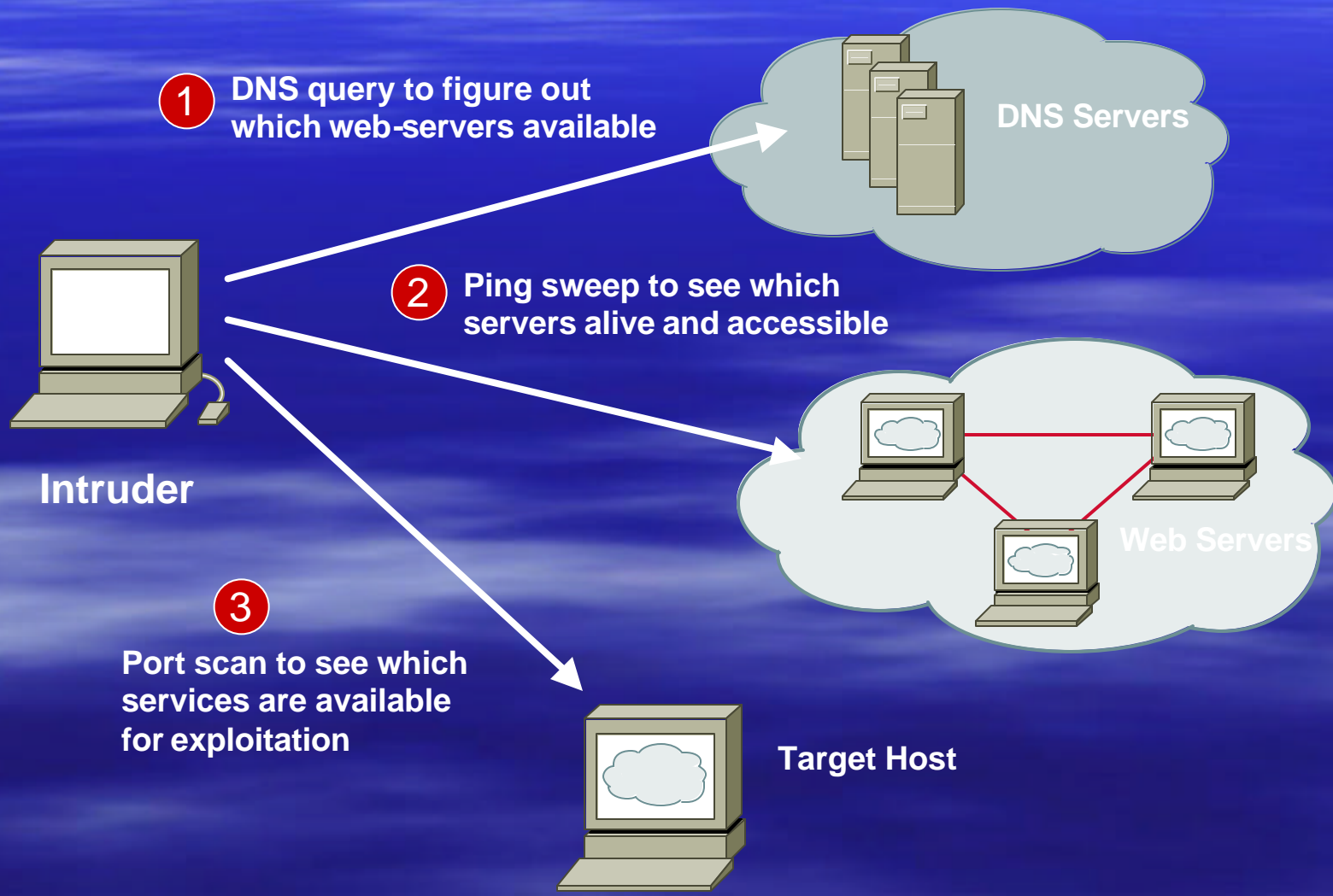
Vulnerability: a weakness in a network that can be exploited by a threat.

Types of Network Threats

- Unauthorized Access
 - Eavesdropping/Port scanning/War dialing
- Impersonation
 - Spoofing attacks/Replay attacks
- Data Manipulation
- Denial of Service (DoS) / DDoS
- Viruses
- Email SPAM

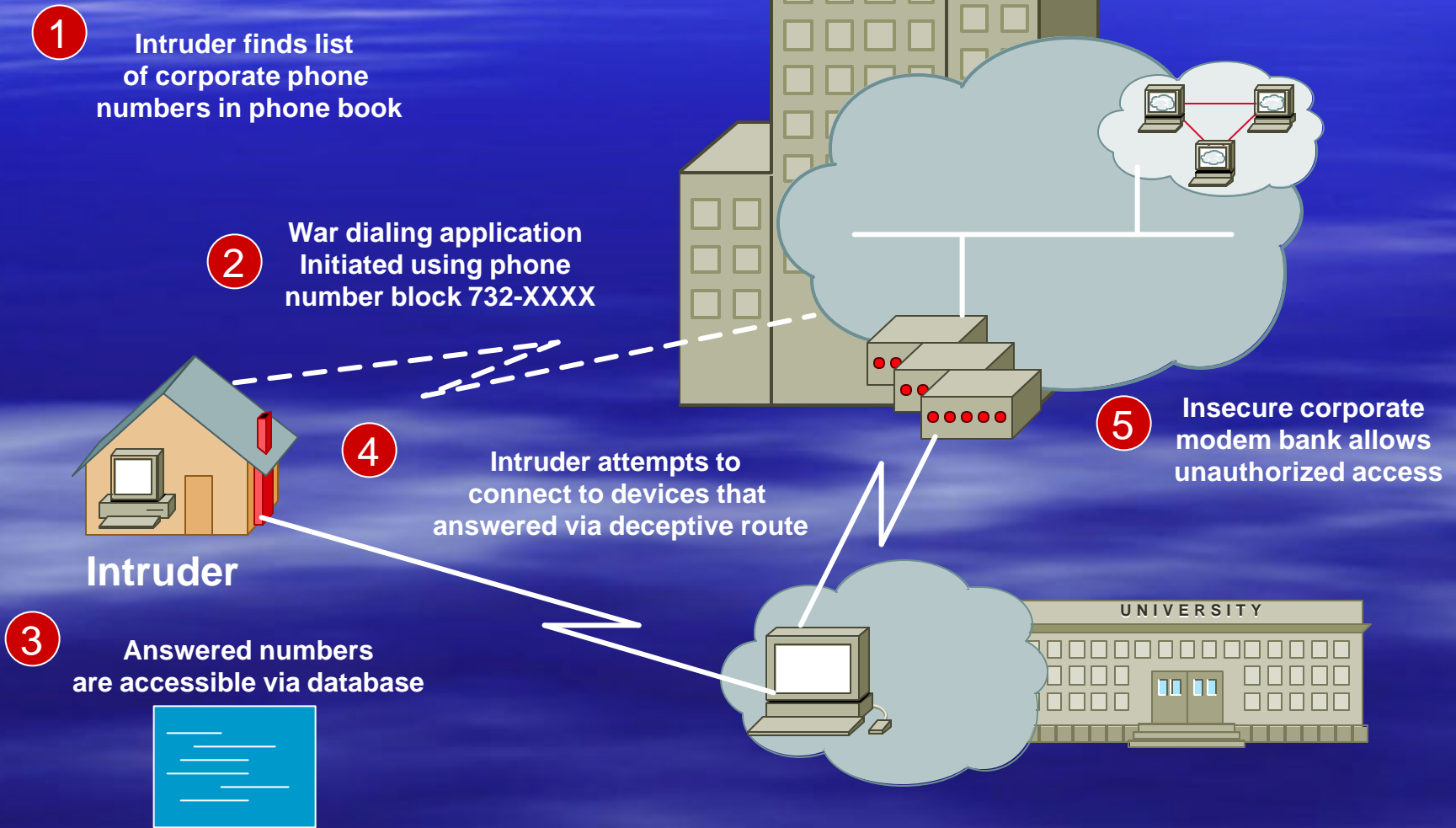
Which are you susceptible to ?!?!?

Example Reconnaissance Attempt



War Dialing

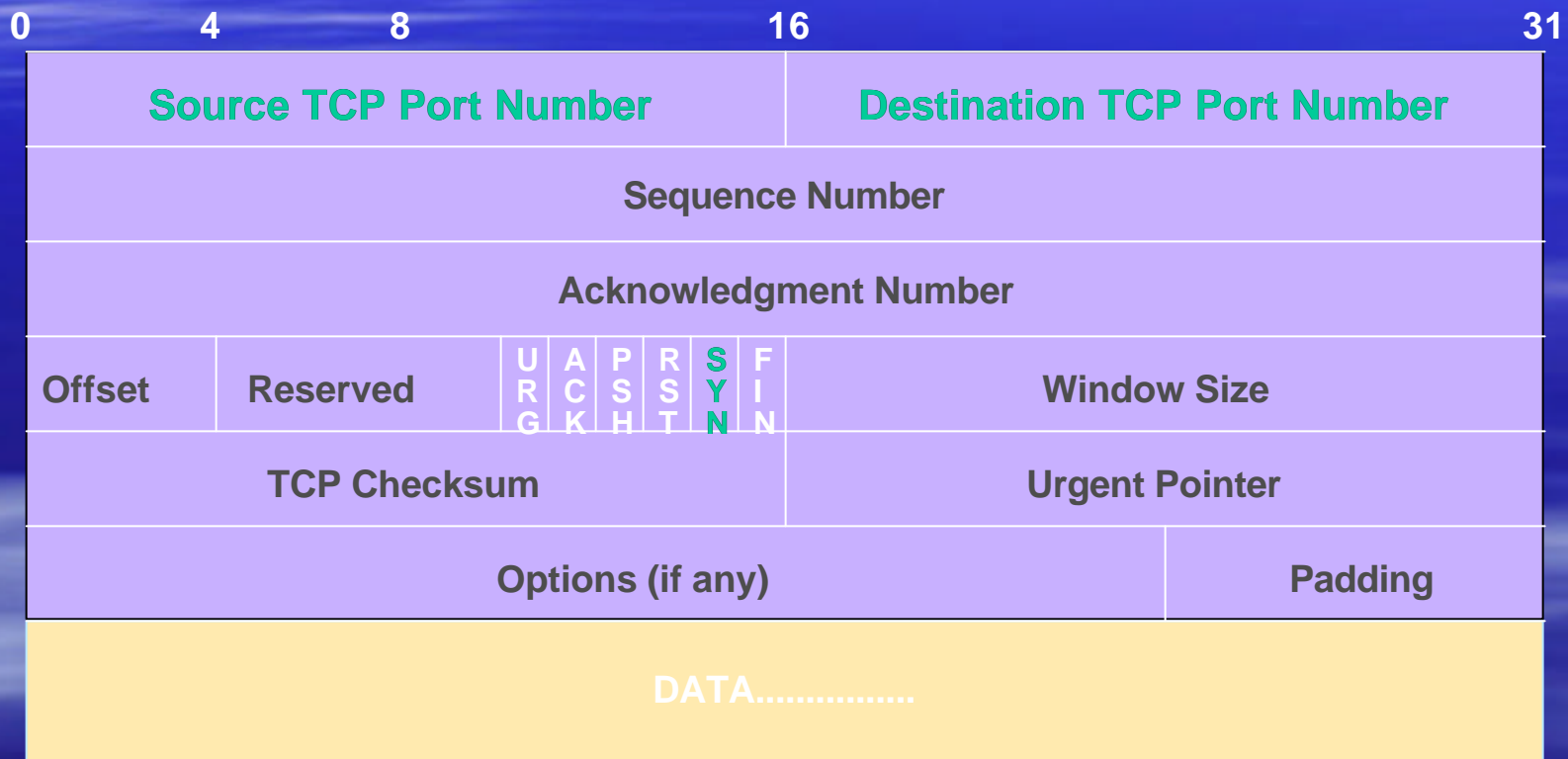
Large Interesting Corporation



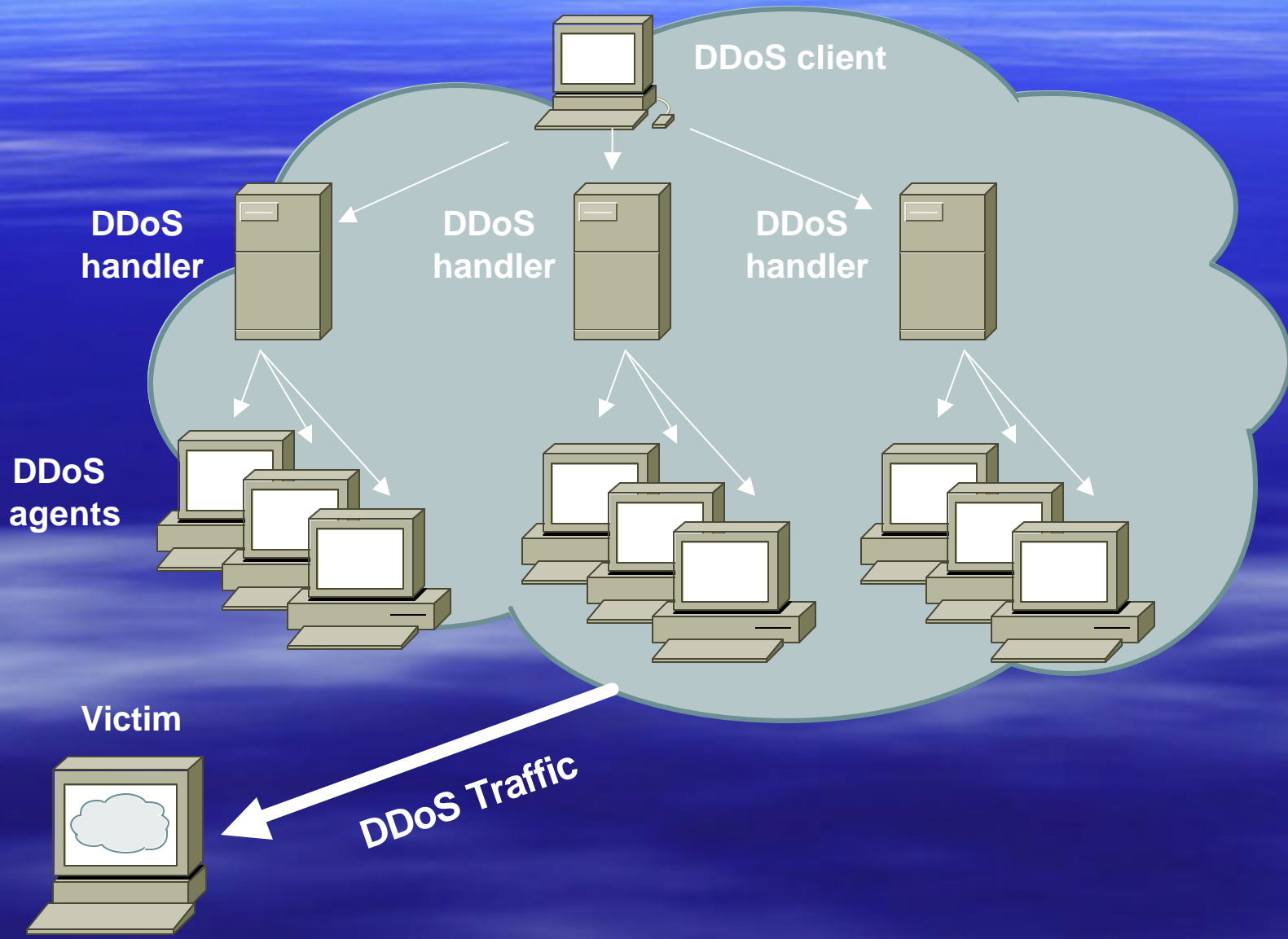
DoS and DDoS Attacks

- TCP SYN
- TCP ACK
- UDP, ICMP, TCP floods
- Fragmented Packets
- IGMP flood
- Spoofed and un-spoofed

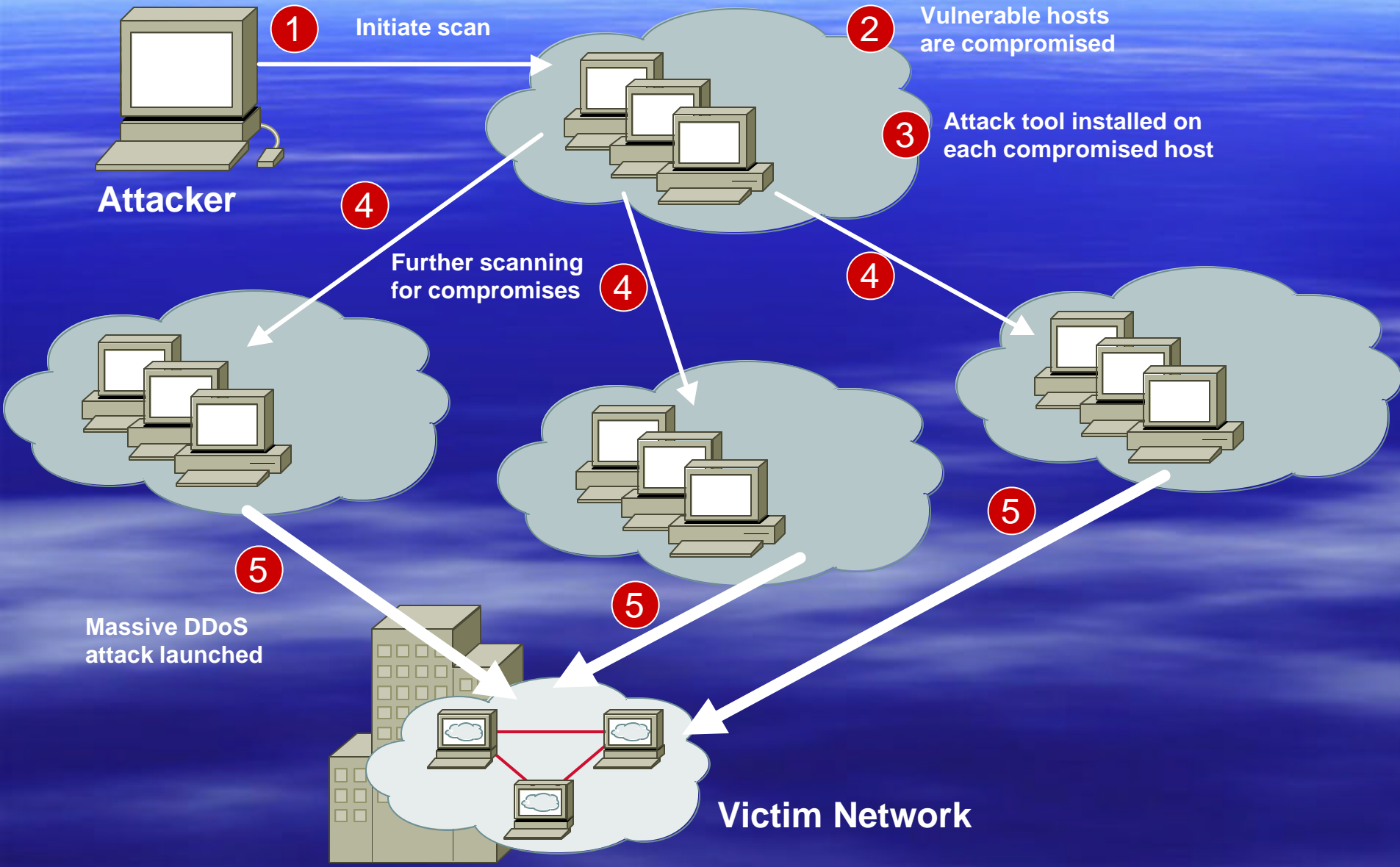
TCP Packet Format



Basics of a DDoS Attack



Automated DDoS Attack



DDoS Vulnerabilities

- Distributed and/or coordinated attacks
 - Increasing rate and sophistication
- Infrastructure protection
 - Coordinated attack against infrastructure
 - Attacks against multiple infrastructure components
- Overwhelming amounts of data
 - Huge effort required to analyze
 - Lots of uninteresting events

What If Router Becomes Attack Target?

It allows an attacker to:

- Disable the router & network...
- Compromise other routers...
- Bypass firewalls, IDS systems, etc...
- Monitor and record all outgoing and incoming traffic...
- Redirect whatever traffic they desire...

Router CPU Vulnerabilities

CPU Overload

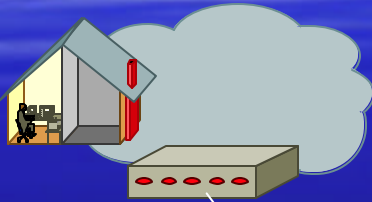
- Attacks on applications on the Internet have affected router CPU performance leading to some BGP instability
- 100,000+ hosts infected with most hosts attacking routers with forged-source packets
- Small packet processing is taxing on many routers...even high-end
- Filtering useful but has CPU hit

Router Security Considerations

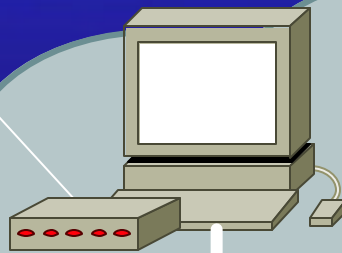
- Segment areas for route redistribution and ensure limited access to routers in critical backbone areas
- Design networks so outages don't affect entire network but only portions of it
- Control router access....watch against internal attacks on these systems. Use different passwords for router enable and monitoring system root access.
- Latest scanning craze for http access!!!

What Is Wrong Here?

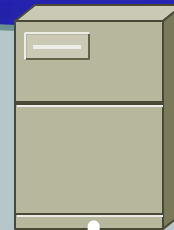
House with Computer



Workstation with Modem

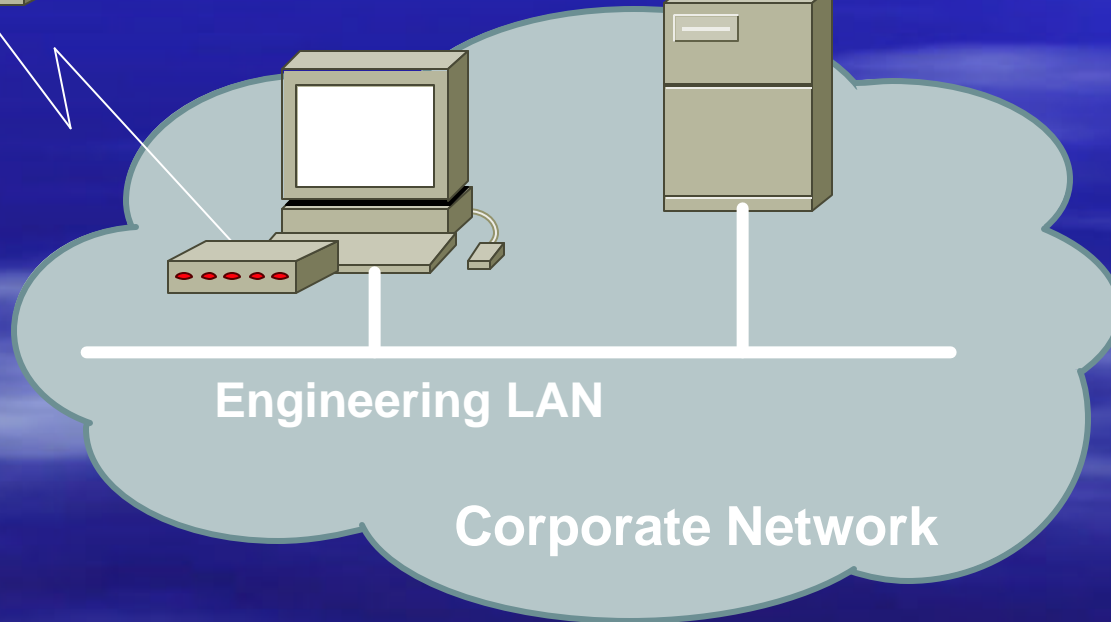


Secure Engineering Server



Engineering LAN

Corporate Network



How Do You Secure Infrastructure ?

- **Securing Infrastructure Devices**
- Routing Protocol Security
- Securing the Network Perimeter (Edge)
- Securing Remote Access
- Mitigating DDoS Attacks

Infrastructure Device Integrity

- Who has physical access?
- Who has logical access?
- What is confidential?



Device Access Security

- Physical Location
 - Limit physical access to devices
- Logical Access
 - Console Access
 - How is it authenticated?
 - How long before timeout?
 - Virtual Terminal Access
 - How is it authenticated?
 - How long before timeout?
 - Specify specific hosts?

Secure Configurations

- Secure console and virtual terminal access
 - Simple clear-text password (YUK!!)
 - TACACS+/RADIUS with clear-text or token card
 - SSH
 - Kerberos v5
- Multiple privilege levels for configuration and user commands
- Encrypted passwords when viewing configurations

Do NOT Even Think of Using Telnet

- Telnet is a bad idea!
- Avoid it from the start
- Telnet sends username and password information across the wire in plain text format.
- Do not use telnet to gain access to any of your boxes (router-to-router could be exception for troubleshooting, but limit access in these instances)

SSH

- Two flavors of ssh, ssh1 and ssh2
- Use ssh2 if possible
- In general the client connecting to your ssh server will either "speak" ssh1 or ssh2
- Openssh from <http://www.openssh.org/> this can support both
- ssh has the advantage that username and password information is sent across the line encrypted and it is non-trivial to break this encryption

Example – NOT Very Secure

```
service password-encryption
enable secret 5 $1$mgfc$ISYSLeC6ookRSV7sI1vXR.
enable password 7 075F701C1E0F0C0B
!
username staff password 7
104F0B0A0A1B071F5D547A

line con 0
!
line vty 0 4
exec-timeout 0 0
login local
transport input telnet
```

Banner....what's wrong?

banner login ^C
Martini

2.5 ounces vodka
1/5 ounce dry vermouth

Fill mixing glass with ice, add vermouth and vodka, and stir to chill. Strain into a Martini glass and garnish with an olive or lemon twist.

RELAX....INDULGE.....Get Off My Router!!

^C

Better Device Banner

!!!! WARNING !!!!

You have accessed a restricted device.

All access is being logged and any
unauthorized access will be
prosecuted to the full extent of the
law.

Device Integrity Checklist

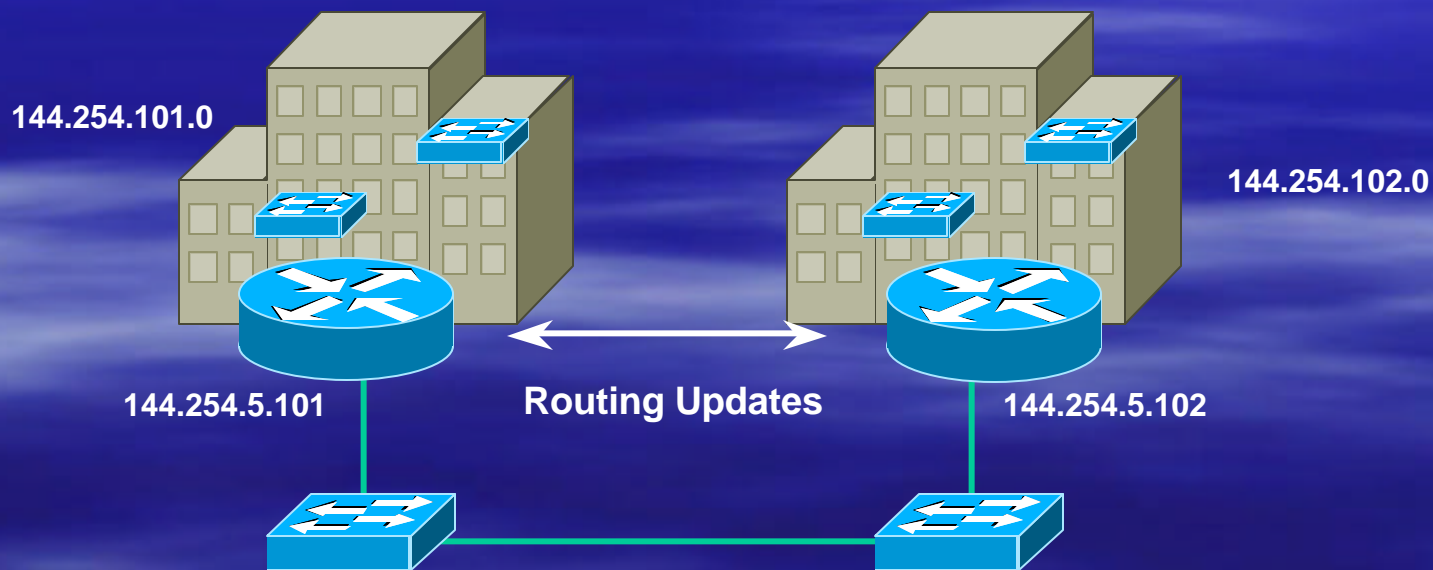
- Secure logical access to routers with passwords and timeouts
- Restrict logical access to specified trusted hosts
- Never leave passwords in clear-text
- Shut down unused interfaces
- Shut down unneeded services
- Test device integrity on a regular basis

How Do You Secure Infrastructure ?

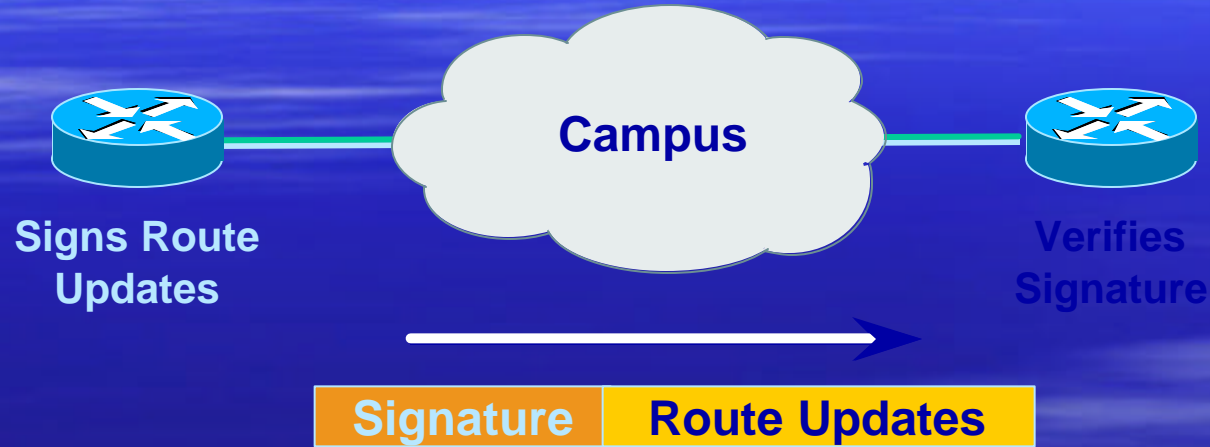
- Securing Infrastructure Devices
- **Routing Protocol Security**
- Securing the Network Perimeter
- Securing Remote Access
- Mitigating DDoS Attacks

Securing Router-to-Router Communication

- Route authentication
- Routing filters
- Encryption

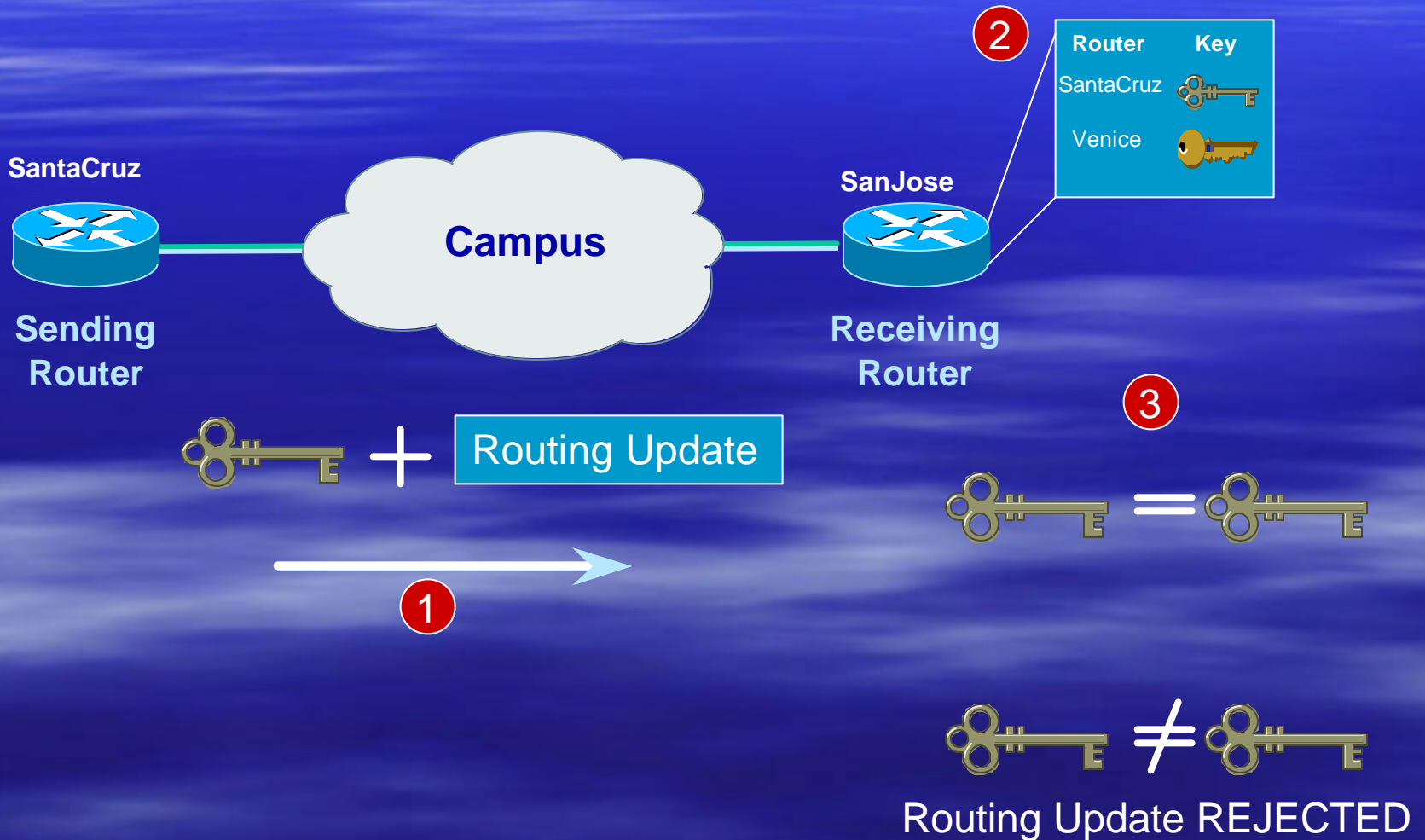


Route Authentication

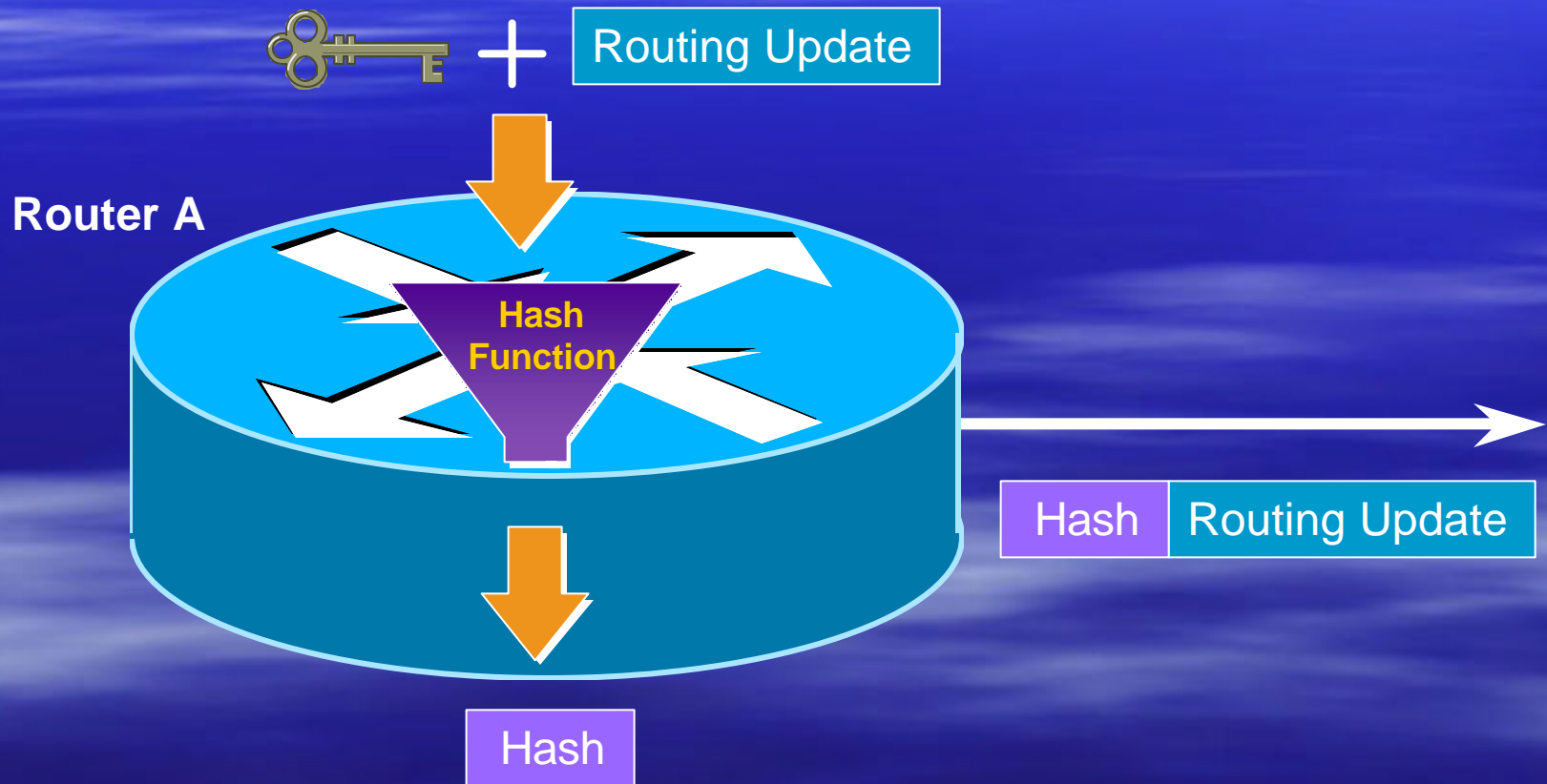


**Certifies authenticity of neighbor
and integrity of route updates**

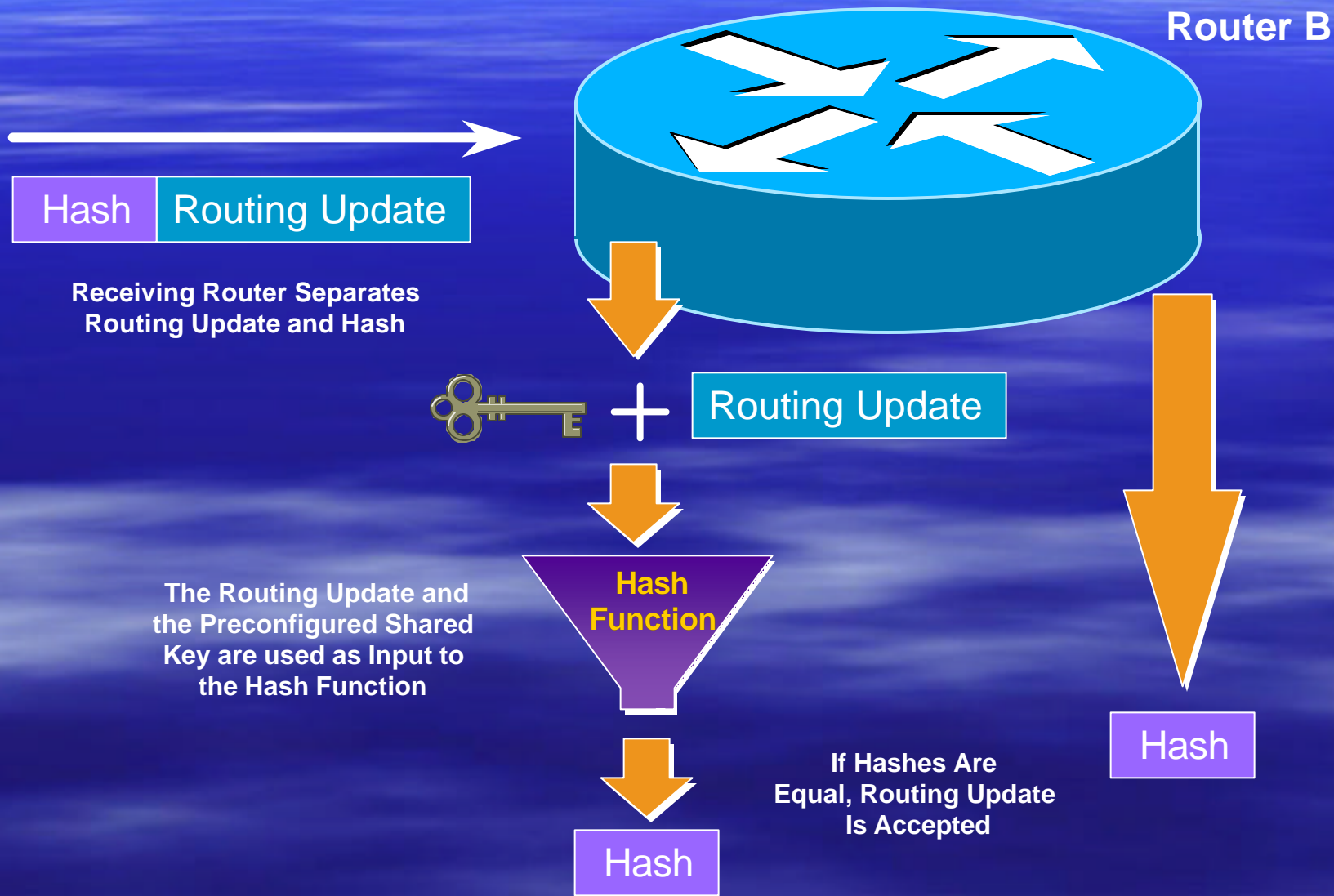
Plaintext Neighbor Authentication



MD-5 Neighbor Authentication: Originating Router



MD-5 Neighbor Authentication: Receiving Router



Routing Security Summary

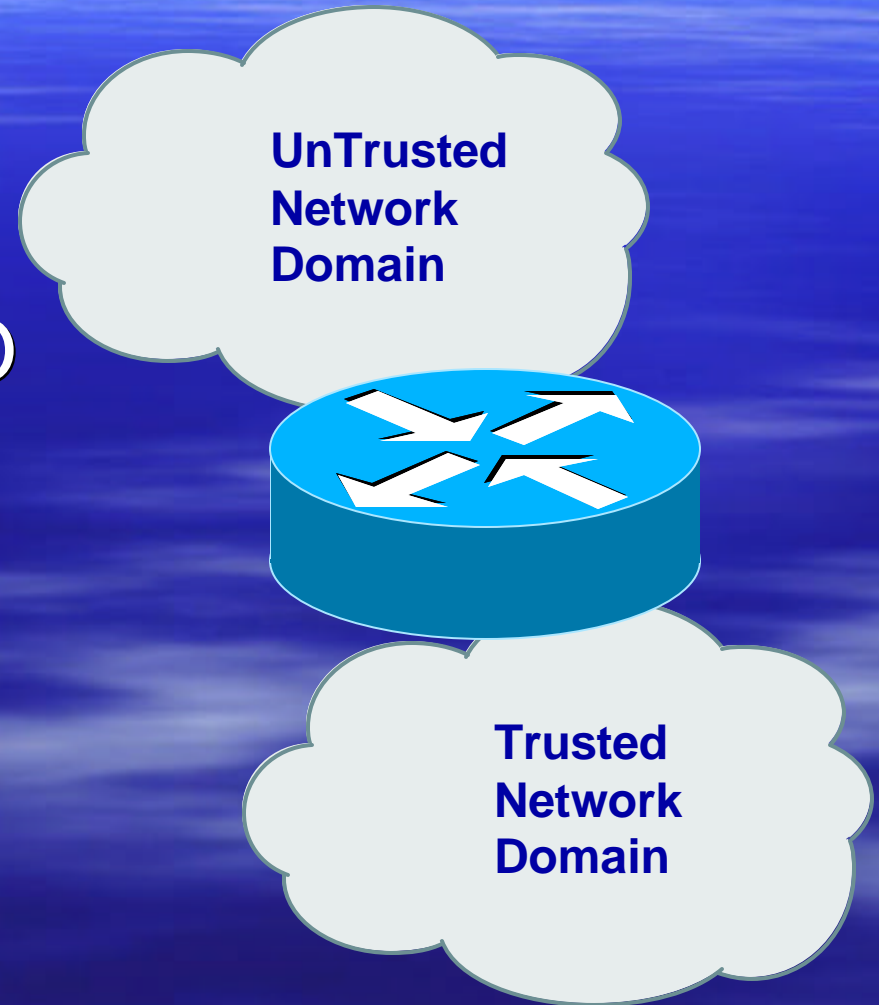
- Always turn on MD5 authentication
- Always filter routing updates....
especially be careful of redistribution
- How paranoid are you?
 - Specify which neighbors are allowed to speak to each other

How Do You Secure Infrastructure ?

- Securing Infrastructure Devices
- Routing Protocol Security
- **Securing the Network Perimeter**
- Securing Remote Access
- Mitigating DDoS Attacks

Role of the Router

- Forwards packets at network layer
- First point of entry TO a trusted network domain
- Last point of exit FROM a trusted network domain



RFC2827 – Ingress Filtering

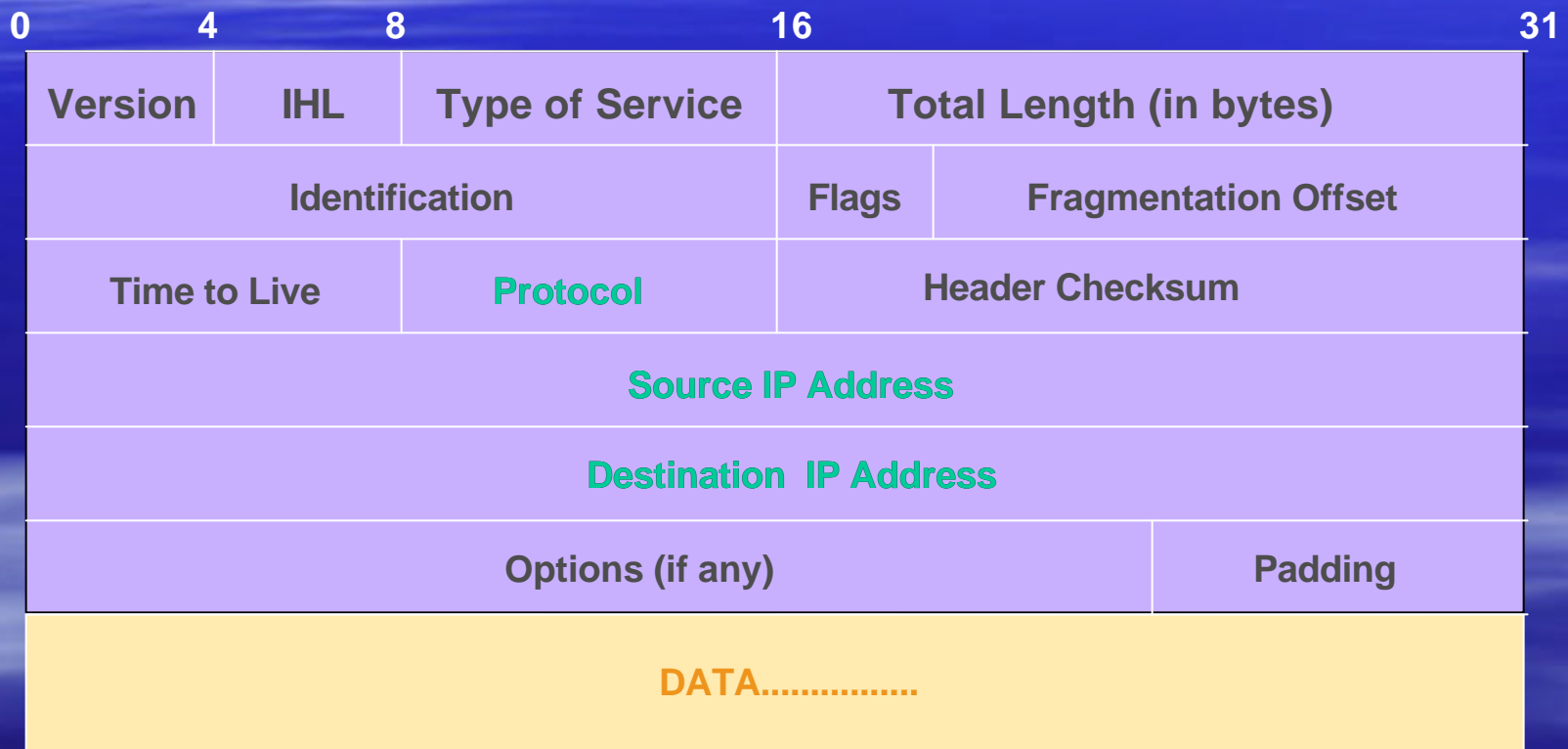
If an ISP is aggregating routing announcements for multiple downstream networks, strict traffic filtering should be used to prohibit traffic which claims to have originated from outside of these aggregated announcements.

RFC2827 – Ingress Filtering

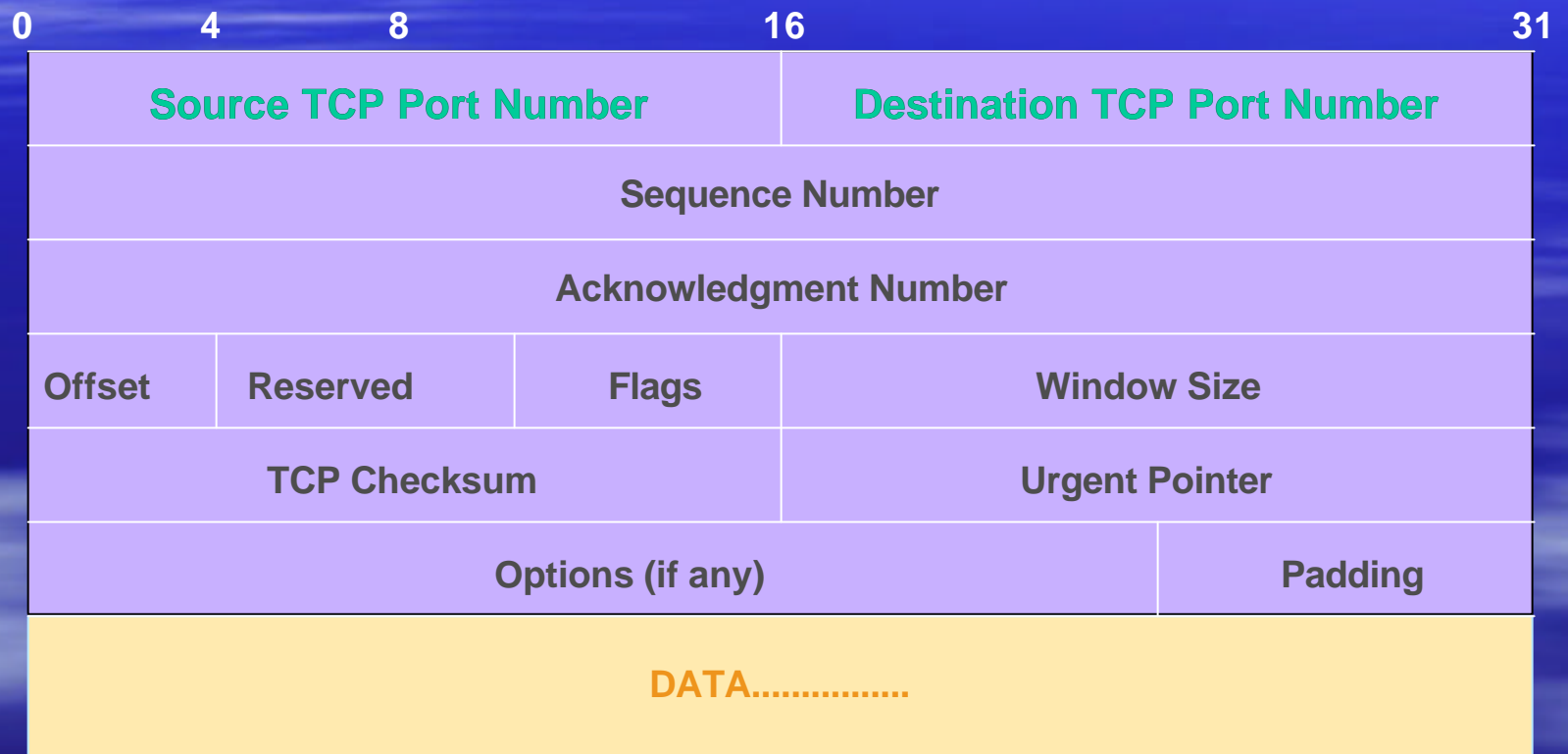
The ONLY valid source IP address for packets originating from that PC is the one assigned by the ISP (whether statically or dynamically assigned).

The remote access server could check every packet on ingress to ensure the user is not spoofing the source address on the packets which he is originating.

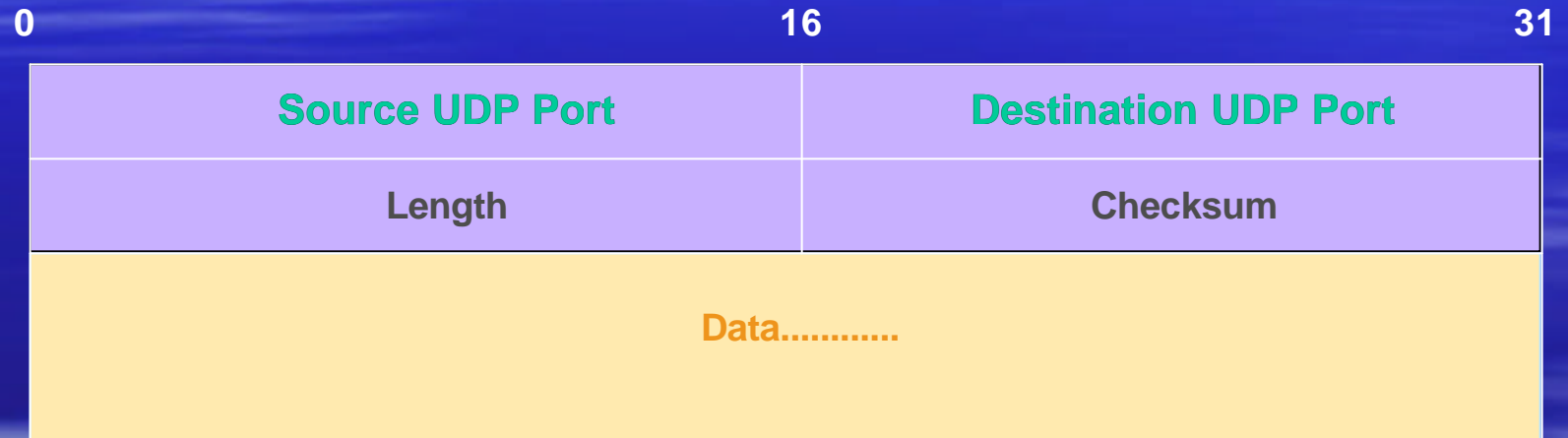
IP Header Format



TCP Header Format



UDP Header Format



Filtering Recommendations

- Log filter port messages properly
- Allow only internal addresses to enter the router from the internal interface
- Block packets from outside (untrusted) that are obviously fake or commonly used for attacks
- Block packets that claim to have a source address of any internal (trusted) network.

Filtering Recommendations

- Block incoming loopback packets and RFC 1918 networks
 - 127.0.0.0
 - 10.0.0.0 – 10.255.255.255
 - 172.16.0.0 – 172.31.0.0
 - 192.168.0.0 – 192.168.255.255
- Block multicast packets (if NOT using multicast)
- Block broadcast packets (careful of DHCP and BOOTP users)
- Block incoming packets that claim to have same destination and source address

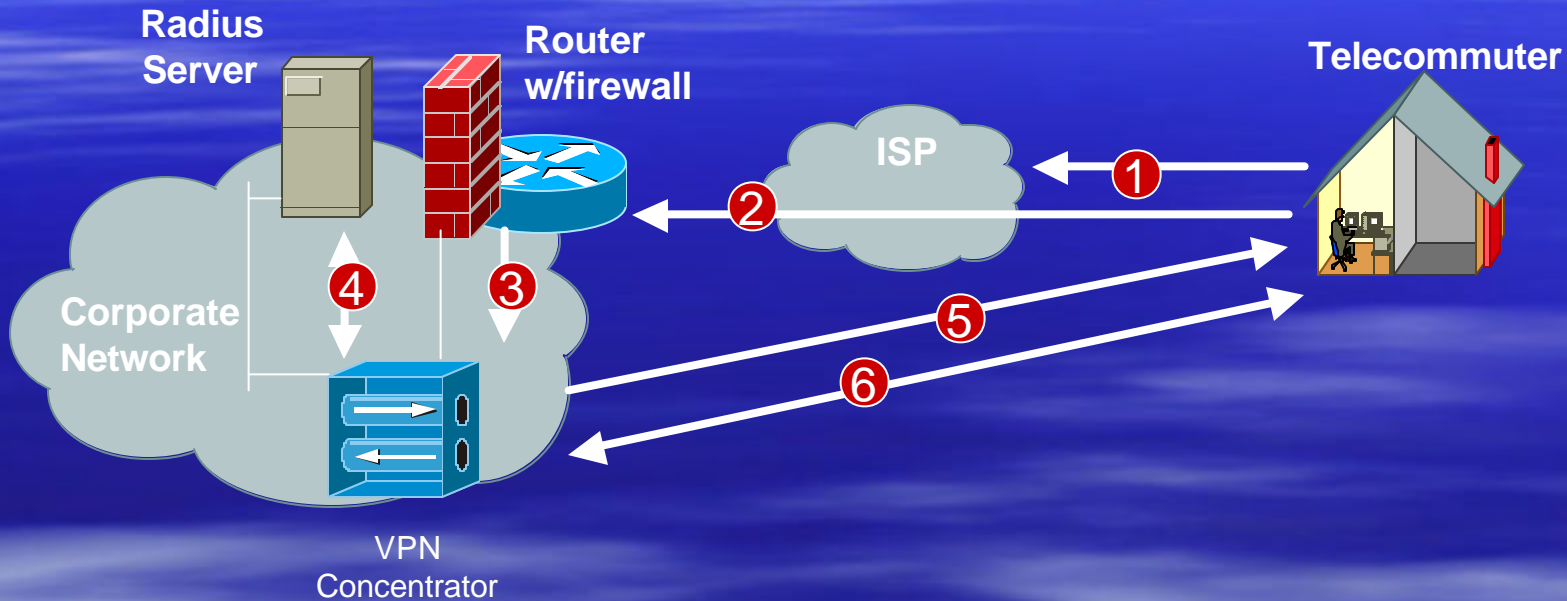
Filtering Issues

- Ordering
 - What sequence is packet inspected in?
- Performance
 - Are there any limitations?
- Logging
 - Get appropriate information
 - Timestamps

How Do You Secure Infrastructure?

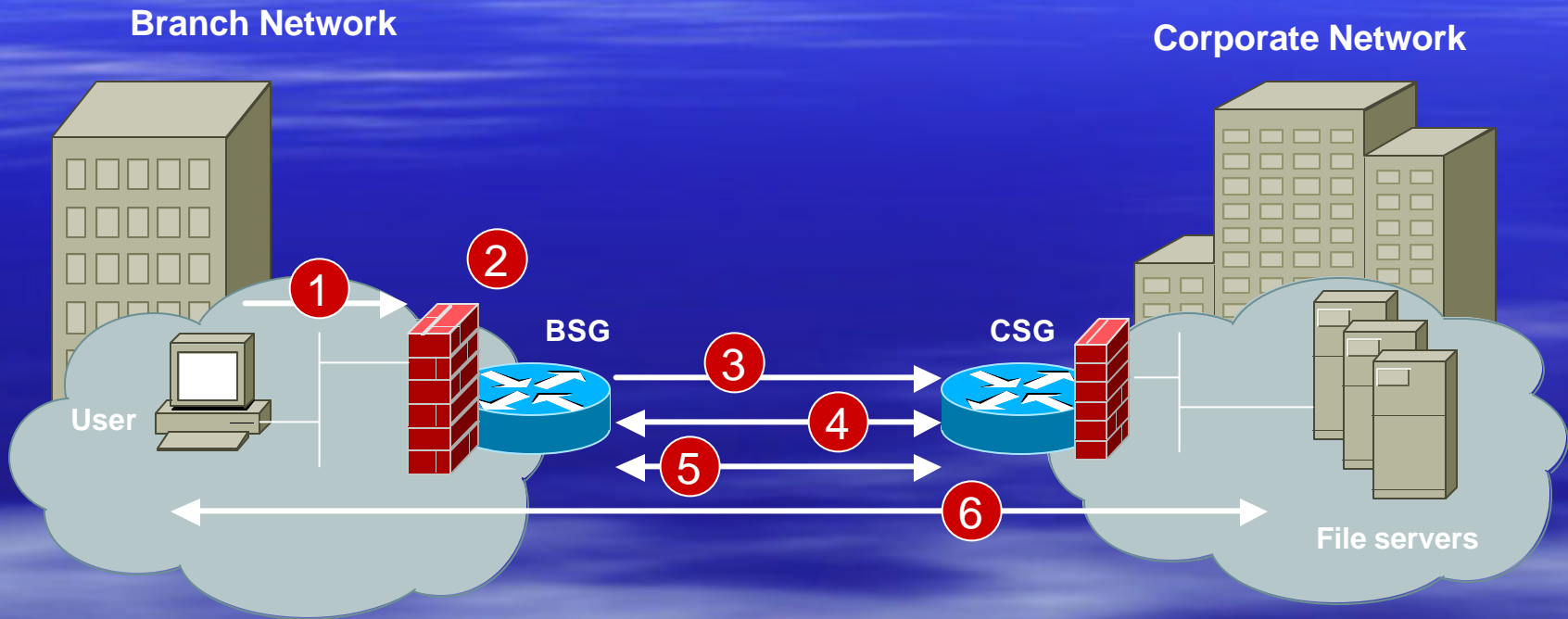
- Securing Infrastructure Devices
- Routing Protocol Security
- Securing the Network Perimeter
- **Securing Remote Access**
- Mitigating DDoS Attacks

Access VPN



SSL or IPsec ?

Intranet VPN



How Do You Secure Infrastructure ?

- Securing Infrastructure Devices
- Routing Protocol Security
- Securing the Network Perimeter
- Securing Remote Access
- **Mitigating DDoS Attacks**

Today's DoS Prevention

- Allow only good traffic into your network (ingress filtering)
- Allow only good traffic out of your network (egress filtering)
- Stop directed broadcast traffic (to avoid being an amplifier)

Deny all and permit only what's needed is most effective policy

DoS Filtering

Description	Network
default	0.0.0.0 /8
loopback	127.0.0.0 /8
RFC 1918	10.0.0.0 /8
RFC 1918	172.16.0.0 /12
RFC 1918	192.168.0.0 /16
Net Test	192.0.2.0 /24
Testing devices	192.18.0.0 /15
IPv6 to IPv4 relay	192.88.99.0 /24
RFC 1918 nameservers	192.175.48.0 /24
End-node auto configuration	169.254.0.0 /16

Reverse Path Forwarding

- Ensure input interface is feasible path to source address of incoming packet
- Problematic with asymmetric routing

DoS/DDoS Tools

- Vendor provided
 - Arbor TrafGen
- Open source
 - stream
 - litestorm
 - rc8.o
 - f__kscript
 - slice3

Audit Tools and Incident Handling

- Do you know how to map an IP address to a specific destination?!? (which machine correlates to an IP address)
- Ensure timestamps are valid (NTP sources)
- Log only what's needed....avoid information overload

Data Collection/Correlation

- Collecting data
 - Time correlation, communications, common formatting, etc.
 - These issues are addressed by numerous projects
 - IDEF, IDMEF, CIDF, D-Shield, Incidents.org, etc.
- Correlating data
 - How can we tell what events are related?
 - Attacker's goals determine behavior
 - Multiple hypothesis tracking

Intrusion Detection Systems

- Two methods of intrusion detection
 - Signature detection (pattern matching)
 - Low false positive / Detects only known attacks
 - Statistical anomaly detection
 - High false positive / Detects wider range of attacks

Signature vs Anomaly Detection

- Modeling signature detection is easy
 - If a known attack occurred in an observable area, then $p(\text{detection}) = 1$, else $p(\text{detection}) = 0$
- Modeling anomaly detection is more difficult
 - Noisy and/or unusual attacks are more likely seen
 - Denial of Service, port scans, unused services, etc.
 - Other types of attacks may be missed
 - Malformed web requests, some buffer overflows, etc.

Bypassing IDS Systems

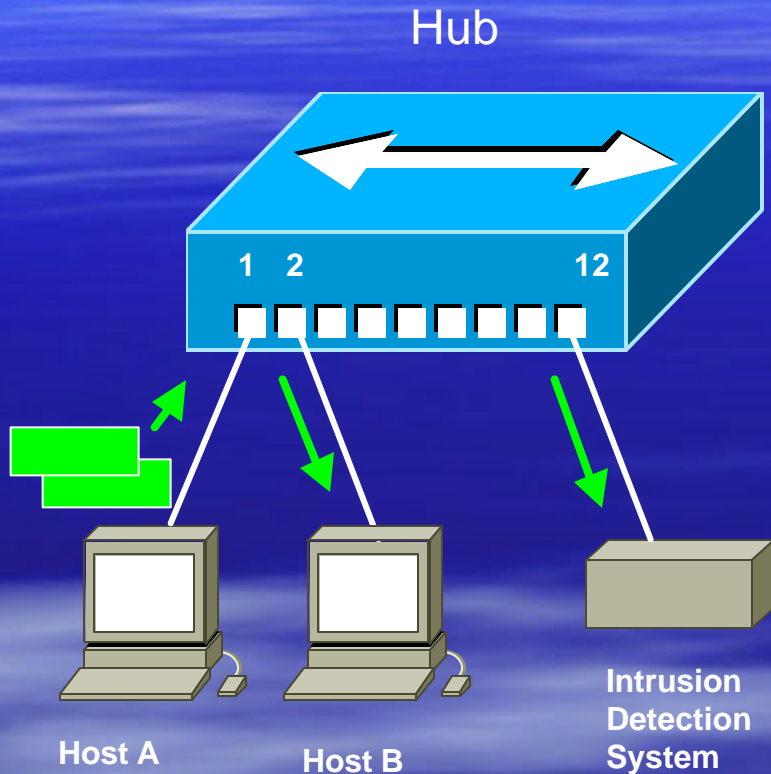
- How varying TCP/IP stacks behave to slightly invalid input.
 - send TCP options, cause timeouts to occur for IP fragments or TCP segments
 - overlap fragments/segments
 - send slight wrong values in TCP flags or sequence numbers.

[If overlapping fragments are sent with different data, some systems prefer the data from the first fragment (WinNT, Solaris), whereas others keep the data from the last fragment (Linux, BSD). The NIDS has no way of knowing which the end-node will accept, and may guess wrong.]

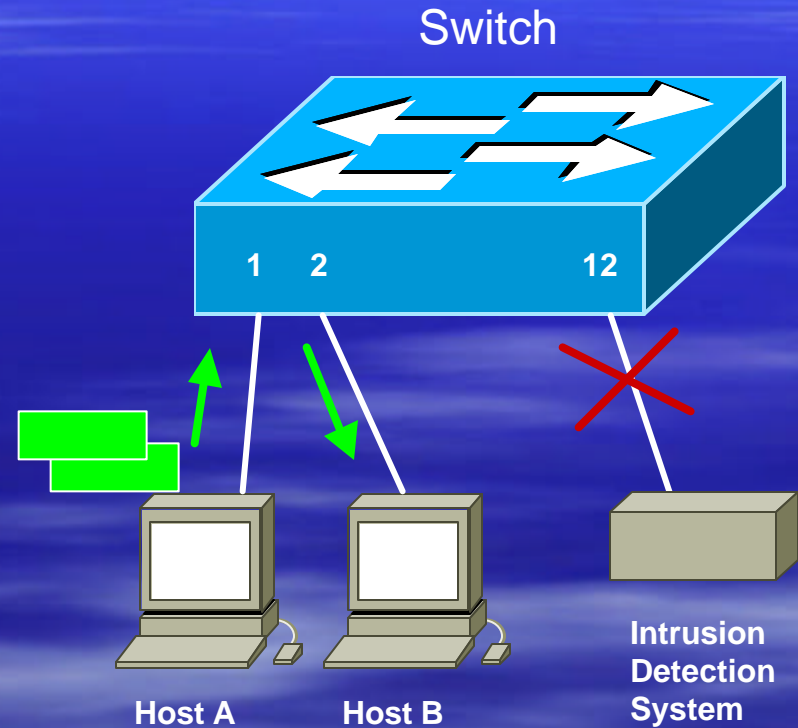
IDS Limitations

- Vern Paxson's USENIX presentation in 1998 on 'Bro - A system for Detecting Network Intruders in real Time'
<ftp://ftp.ee.lbl.gov/papers/bro-usenix98-revised.ps.Z>
- Thomas H. Ptacek and Timothy N. Newsham., "Insertion, Evasion, And Denial Of Service: Eluding Network Intrusion Detection," Technical Report, Secure Networks, Inc., January 1998.
<http://citeseer.nj.nec.com/ptacek98insertion.html>

Hub vs Switch with IDS

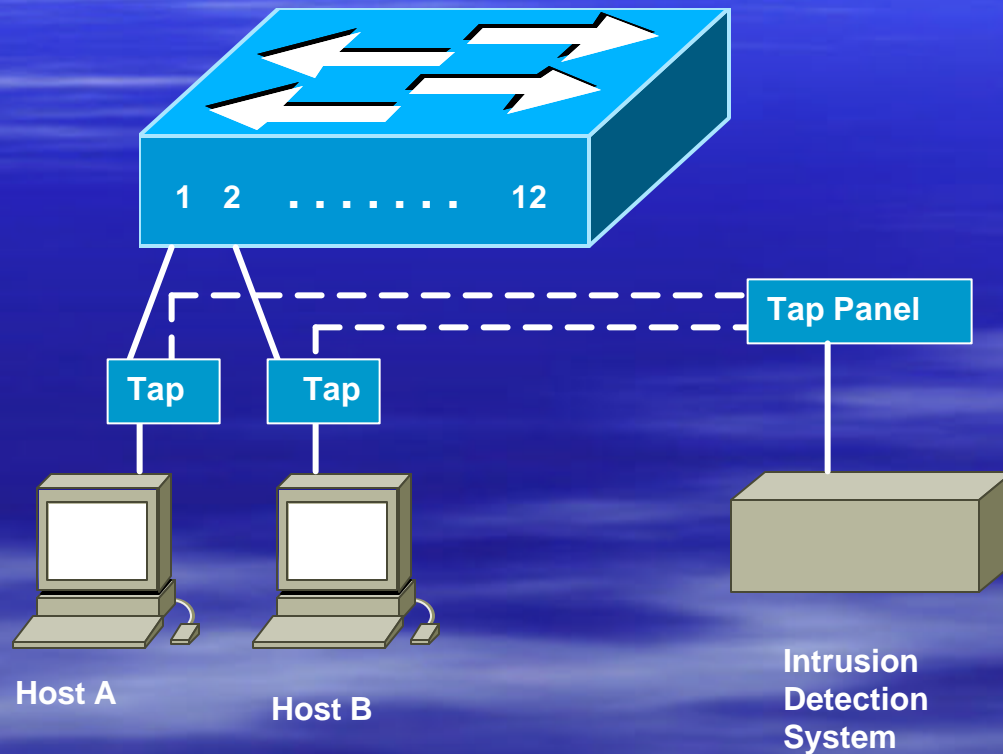


Traffic from host A to host B gets sent to **all** hub ports so the IDS can effectively monitor the traffic.



Traffic from host A to host B gets sent only to the port which connects host B and the IDS does not see any traffic.

Using NIDS with Cable Taps



Collecting Incident Data

Traditional Forensics

- Immediately shutdown the system (or pull the power cord)
- Make a forensic duplicate
- Perform analysis on the duplicate
- Live system data is rarely recovered.

Infrastructure Forensics

- Live system data is the most valuable.
- Immediate shutdown destroys all of this data.
- Persistent (flash) data will likely be unchanged and useless.
- Investigators must recover live data for analysis

Bare Minimum Device Security

- Authenticate and keep track of who has accessed infrastructure devices
- Configure access remotely only through ssh or trusted hosts (know what data is sent in the clear)
- Disable access that is not used
- Accurate timestamps for all logging
- Keep keys confidential

Not To Be Forgotten

- DNS Servers

- Lame delegations are evil

- Recursive DNS can lead to cache poisoning (UDP – trivial to determine seq# and create invalid entry)

- Block traffic to destination port 53 only and allow traffic to source port 53 that already has an established connection

- Email Servers

- Spam attacks and deterrents:

- <http://spam.abuse.net/>

- <http://www.cauce.org/>

Agenda

- Session I (1:30 – 3:00)
Security Technology Details
- Session II (3:30 – 5:00)
Secure Infrastructure Architectures
- **Session III (7:30 – 9:00)**
Sample Configuration Scenarios

What Do I Configure

- Device Security
- Filtering
- Routing Security
- IPsec
- DoS/DDoS Mitigation
- Incident Response

Generic Device Security Checklist

- Console access
- Logical access
 - telnet vs ssh
 - http
 - snmp
- Logging
- Encrypting Passwords

Device Security Checklist (Layer 3)

- Blackhole Filtering
- Routing Authentication
- ICMP Filters
- Other filtering templates

Device Security Checklist (Layer 2)

- MAC Filters
- Port Authentication – 802.1x

What Do I Configure

- Device Security
- Filtering
- Routing Security
- IPsec
- DoS/DDoS Mitigation
- Incident Response

Making IPsec Configuration Understandable

- Vendors have made it hard since no collaboration for defaults (even within same company)
- YOU need to define appropriate options

Pretty Good IPsec Policy

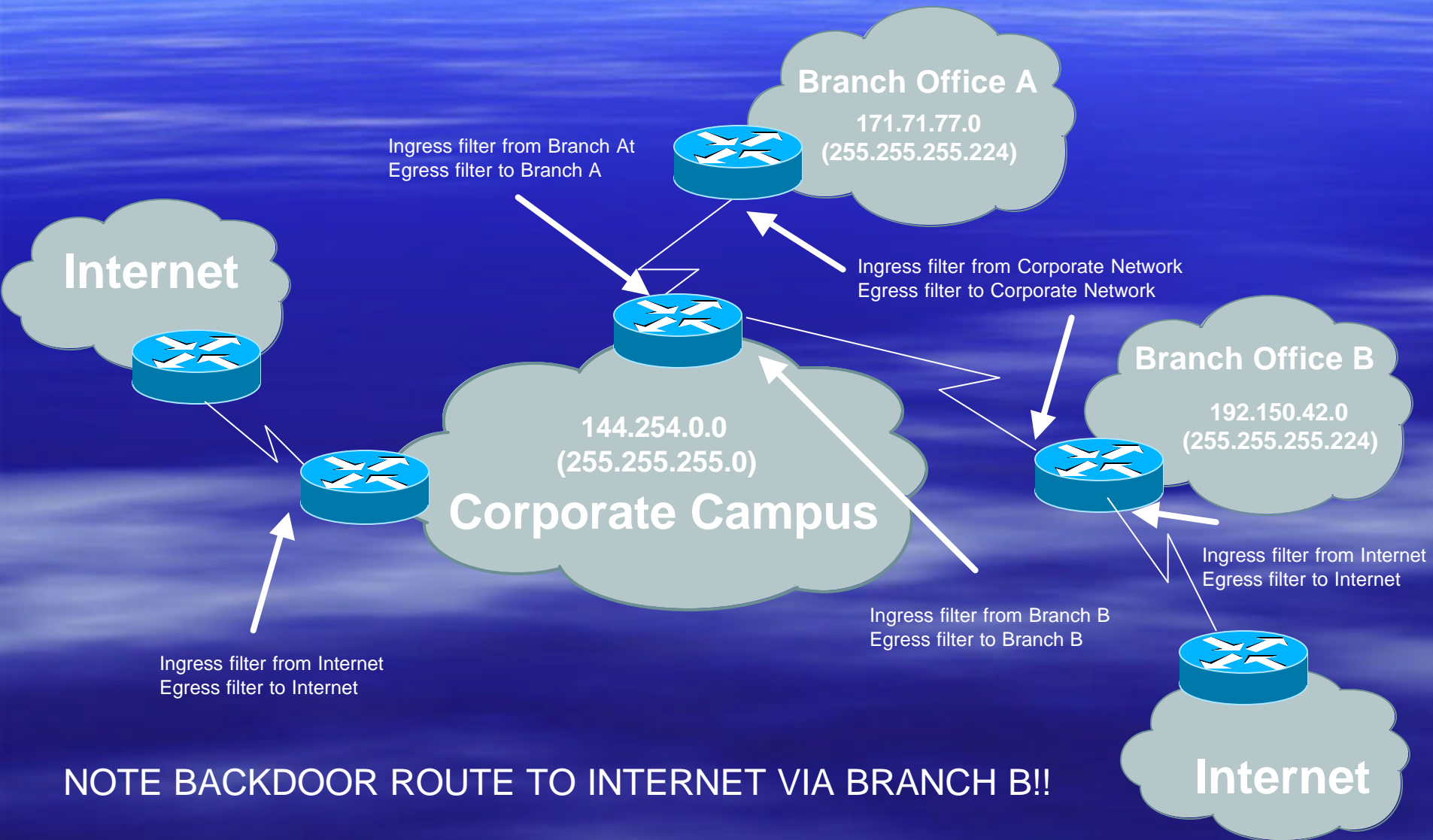
- IKE Phase 1 (aka ISAKMP)
 - 3DES
 - Lifetime (how many seconds in 1 day?)
 - SHA-1
 - DH Group 2 (MODP)
- IKE Phase 2 (aka IPsec)
 - 3DES
 - Lifetime (how many seconds in 1 hour?)
 - SHA-1
 - PFS
 - DH Group 2 (MODP)

PFS- what is it?

- Perfect Forward Secrecy
- Doing new DH exchange to derive keying material

(DH used to derive shared secret which is used to derive keying material for IPsec security services)

Advanced Filtering Example



Branch Router Configuration

The configuration is as follows: (for branch A router)

```
access-list 133 deny ip host 0.0.0.0 any
access-list 133 deny ip 127.0.0.0 0.255.255.255 any
access-list 133 deny ip 10.0.0.0 0.255.255.255 any
access-list 133 deny ip 172.16.0.0 0.15.255.255 any
access-list 133 deny ip 192.168.0.0 0.0.255.255 any
access-list 133 deny ip 192.0.2.0 0.0.0.255 any
access-list 133 deny ip 169.254.0.0 0.0.255.255 any
access-list 133 deny ip 240.0.0.0 15.255.255.255 any
access-list 133 deny ip 171.71.32.0 0.0.0.31 any
access-list 133 permit ip any any
```

```
access-list 144 permit ip 171.71.32.0 0.0.0.31 any
access-list 144 deny ip any any
```

```
interface BRI0
description To Corporate Network
ip access-group 133 in
ip access-group 144 out
```

NAS Router Policy

Ingress filtering:

- permit only traffic with an IP source address of branch networks
- deny all other traffic

Egress filtering:

- deny all rfc 1918 and special use addresses from propagating to branch networks
- deny all traffic with an IP source address that matches the branch network address allocation
- permit all other traffic

NAS Router Configuration

```
access-list 133 permit ip 171.71.32.0 0.0.0.31 any
access-list 133 permit ip 192.150.42.0 0.0.0.31 any
access-list 133 deny ip any any
```

```
access-list 144 deny ip host 0.0.0.0 any
access-list 144 deny ip 127.0.0.0 0.255.255.255 any
access-list 144 deny ip 10.0.0.0 0.255.255.255 any
access-list 144 deny ip 172.16.0.0 0.15.255.255 any
access-list 144 deny ip 192.168.0.0 0.0.255.255 any
access-list 144 deny ip 192.0.2.0 0.0.0.255 any
access-list 144 deny ip 169.254.0.0 0.0.255.255 any
access-list 144 deny ip 240.0.0.0 15.255.255.255 any
access-list 144 deny ip 171.71.32.0 0.0.0.31 any
access-list 144 deny ip 192.150.42.0 0.0.0.31 any
access-list 144 permit ip any any
```

```
interface Serial 0:23
description To Branch Offices
ip access-group 133 in
ip access-group 144 out
```


Internet Router Policy

Ingress filtering:

- deny all rfc 1918 and special use addresses from entering the corporate network
- deny all traffic with an IP source address of the corporate network or branch networks
- permit all other traffic

Egress filtering:

- permit only traffic with an IP source address of the corporate network and branch networks
- deny all other traffic

Internet Router Configuration

```
access-list 133 deny ip host 0.0.0.0 any
access-list 133 deny ip 127.0.0.0 0.255.255.255 any
access-list 133 deny ip 10.0.0.0 0.255.255.255 any
access-list 133 deny ip 172.16.0.0 0.15.255.255 any
access-list 133 deny ip 192.168.0.0 0.0.255.255 any
access-list 133 deny ip 192.0.2.0 0.0.0.255 any
access-list 133 deny ip 169.254.0.0 0.0.255.255 any
access-list 133 deny ip 240.0.0.0 15.255.255.255 any
access-list 133 deny ip 144.254.0.0 0.0.255.255 any
access-list 133 deny ip 171.71.32.0 0.0.0.31 any
access-list 133 deny ip 192.150.42.0 0.0.0.31 any
access-list 133 permit ip any any
```

```
access-list 144 permit ip 144.254.0.0 0.0.255.255 any
access-list 144 permit ip 171.71.32.0 0.0.0.31 any
access-list 144 permit ip 192.150.42.0 0.0.0.31 any
access-list 144 deny ip any any
```

```
interface Serial 0/0
description To Internet
ip access-group 133 in
ip access-group 144 out
```

Session Summary

- Create a usable security policy
- Limit access to infrastructure devices
- Provide good levels of authentication (ssh, one-time-password)
- FILTER at the EDGE
- Use route authentication
- Audit your network infrastructures

Configuring IPsec

STEP 1 *Configure the IKE Phase 1 Policy (ISAKMP Policy)*

Cisco literature refers to IKE Phase 1 as the ISAKMP policy. It is configured using the command:

```
crypto isakmp policy priority
```

Multiple policies can be configured and the priority number, which ranges from 1 to 10,000, denotes the order of preference that a given policy will be negotiated with an ISAKMP peer. The lower value has the higher priority. Once in the ISAKMP configuration mode, the following parameters can be specified are:

- Encryption Algorithm
- Hash Algorithm
- Authentication Method
- Group Lifetime

Configuring IPsec

STEP 2 *Set the ISAKMP Identity*

The ISAKMP identity specifies how the IKE Phase 1 peer is identified, which can be either by IP address or host name.

The command to use is:

```
crypto isakmp identity {IP address | hostname}
```

By default, a peer's ISAKMP identity is the peer's IP address.

If you decide to change the default just keep in mind that it is best to always be consistent across your entire IPsec-protected network in the way you choose to define a peer's identity.

Configuring IPsec

STEP 3 *Configure the IPsec AH and ESP Parameters*

The AH and ESP parameters are configured with the following commands:

```
crypto ipsec transform-set transform-set-name <transform 1> <transform 2>  
mode [tunnel | transport]  
crypto ipsec security-association lifetime seconds seconds
```

Configuring IPsec

STEP 4 *Configure the IPsec Traffic Selectors*

The traffic selectors are configured by defining extended access-lists. The *permit* keyword causes all IP traffic that matches the specified conditions to be protected by IPsec

STEP 5 *Configure the IKE Phase 2 (IPsec SA) Policy*

This step sets up a crypto map which specifies all the necessary parameters to negotiate the IPsec SA policy. The following commands are required

```
crypto map crypto-map-name seq-num ipsec-isakmp  
match address access-list-id  
set peer [IP address | hostname]  
set transform-set transform-set-name  
set security-association lifetime seconds seconds  
set pfs [group1 | group 2]
```

Configuring IPsec

STEP 6 *Apply the IPsec Policy to an Interface*

The configured crypto map is then applied to the appropriate interface using the crypto map *crypto-map-name* command. It is possible to apply the same crypto map to multiple interfaces. This case would require the use of the command:

```
crypto map crypto-map-name local-address interface-id
```

Using this command, the identifying interface will be used as the local address for IPsec traffic originating from or destined to those interfaces sharing the same crypto map. A loopback interface should be used as the identifying interface.

Additional IPsec Considerations

- What happens when dynamic IP addresses are used?
- How do you authenticate the actual user as well as the device?

Detecting An Incident

- Accounting discrepancies
- Data modification and deletion
- Users complaining of poor system performance
- Atypical traffic patterns
- Atypical time of system use
- Large numbers of failed login attempts

Incident Response

- DO NOT REBOOT THE DEVICE.
- Change nothing, record everything.
- Before you say it is an accident, make sure it isn't an incident...
- Before you say it is an incident, make sure it isn't an accident...

Incident Response Evidence

Detailed, Methodical, Unquestionable....

- Where you received the evidence...
- When you received the evidence...
- Who you received the evidence from...
- What your seizure methods were...
- Why you seized the evidence...
- How you maintained your chain of custody...

Assessing Damage

- Check log statistics for unusual activity on corporate perimeter network access points, such as Internet access or dial-in access.
- Verify infrastructure device checksum or operating system checksum on critical servers to see whether operating system software has been compromised.
- Verify configuration changes on infrastructure devices and servers to ensure that no one has tampered with them.
- Check sensitive data to see whether it was accessed or changed.
- Check traffic logs for unusually large traffic streams from a single source or streams going to a single destination.
- Run a check on the network for any new or unknown devices.
- Check passwords on critical systems to ensure that they have not been modified (it would be prudent to change them at this point).

Reporting Guidelines

- Keep the technical level of detail low.
- Work with law enforcement officials to ensure that evidence is protected.
- Delegate all handling of the public to in-house PR people who know how to handle the press.
- Do not break or halt lines of communication with the public.
- Keep the speculation out of public statements.
- Do not allow the public attention to detract from the handling of the event.

RFC 3013 (Recommended ISP Security Services & Procedures)

- ISPs have a duty to make sure that their contact information, in Whois, in routing registries [RFC1786] or in any other repository, is complete, accurate and reachable.
- ISPs should have processes in place to deal with security incidents that traverse the boundaries between them and other ISPs.
- ISPs SHOULD be able to conduct such communication over a secure channel.
- ISPs SHOULD be proactive in notifying customers of security vulnerabilities in the services they provide.

RFC 3013 Notifying Customers

Information that should be included:

- who is coordinating response to the incident
- the vulnerability
- how service was affected
- what is being done to respond to the incident
- whether customer data may have been compromised
- what is being done to eliminate the vulnerability
- the expected schedule for response, assuming it can be predicted

THANK YOU!

OK....so I'll plug my book:

Designing Network Security, 2nd Edition
ISBN 1587051176