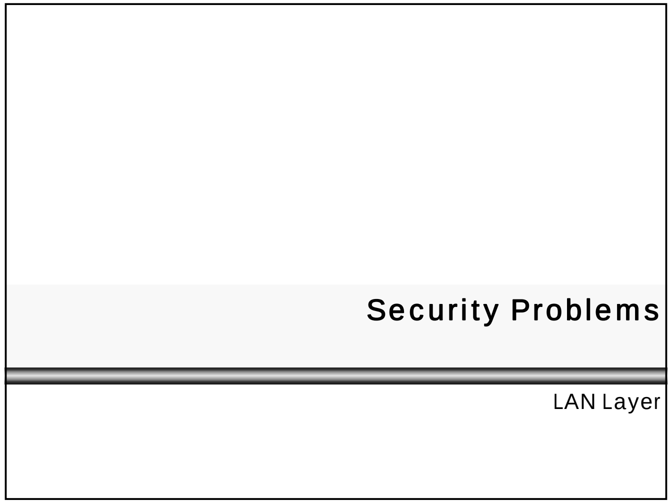
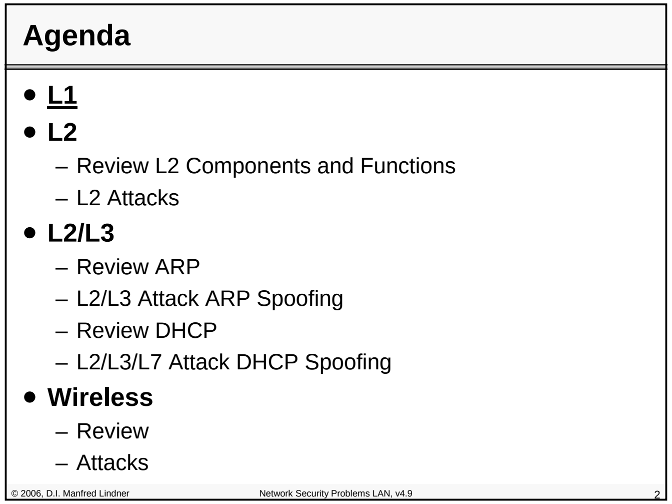


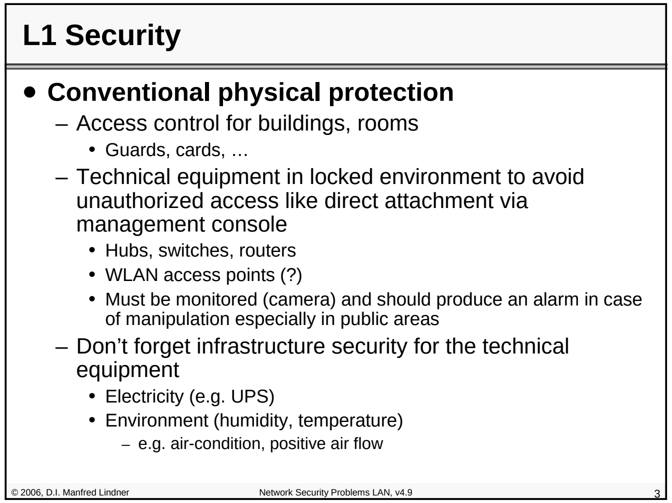
Security Problems

LAN Layer



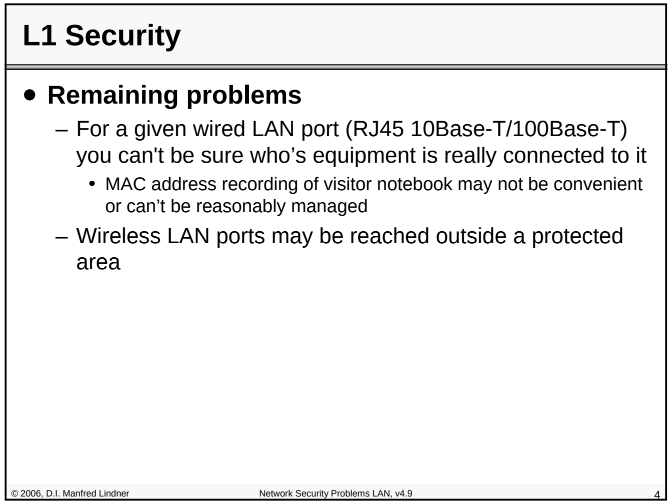
Agenda

- **L1**
- **L2**
  - Review L2 Components and Functions
  - L2 Attacks
- **L2/L3**
  - Review ARP
  - L2/L3 Attack ARP Spoofing
  - Review DHCP
  - L2/L3/L7 Attack DHCP Spoofing
- **Wireless**
  - Review
  - Attacks



L1 Security

- **Conventional physical protection**
  - Access control for buildings, rooms
    - Guards, cards, …
  - Technical equipment in locked environment to avoid unauthorized access like direct attachment via management console
    - Hubs, switches, routers
    - WLAN access points (?)
    - Must be monitored (camera) and should produce an alarm in case of manipulation especially in public areas
  - Don't forget infrastructure security for the technical equipment
    - Electricity (e.g. UPS)
    - Environment (humidity, temperature)
      - e.g. air-condition, positive air flow



L1 Security

- **Remaining problems**
  - For a given wired LAN port (RJ45 10Base-T/100Base-T) you can't be sure who's equipment is really connected to it
    - MAC address recording of visitor notebook may not be convenient or can't be reasonably managed
  - Wireless LAN ports may be reached outside a protected area

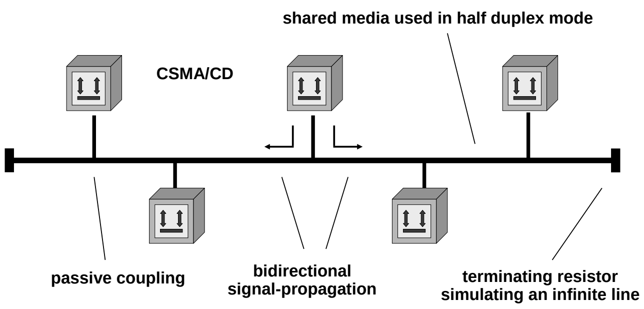
Agenda

- **L1**
- **L2**
  - Review L2 Components and Functions
  - L2 Attacks
- **L2/L3**
  - Review ARP
  - L2/L3 Attack ARP Spoofing
  - Review DHCP
  - L2/L3/L7 Attack DHCP Spoofing
- **Wireless**
  - Review
  - Attacks

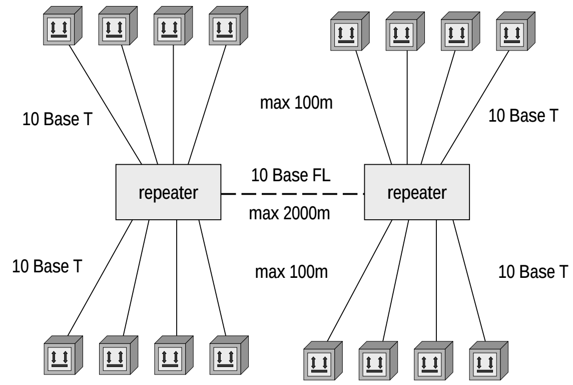
Review L2 Network Components

- **Ethernet**
  - LAN
  - Originally shared media (cable)
  - CSMA/CD as conflict solution if more than one network station access the cable
  - Limited distance
- **Repeater**
  - Amplifier
  - Expansion of LAN
  - Collision domain

Basic Idea of Ethernet


shared media used in half duplex mode
CSMA/CD
passive coupling
bidirectional signal-propagation
terminating resistor simulating an infinite line

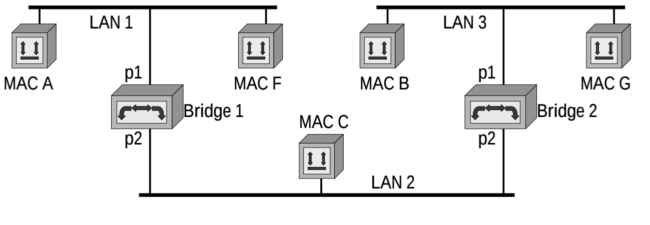
Multiport Repeater as „Hub“



Review L2 Network Components

- **Bridge**
  - Packet switch based on store and forward of frames
  - Bridging table based on MAC addresses
  - “Transparent Bridging”
    - Learning, Forwarding, Filtering, Flooding
  - Broadcast domain
  - “Spanning Tree Protocol” (STP)
- **Ethernet Switch**
  - Fast transparent bridge

Example for Studying Effects



bridging table of bridge 1

p1	p2

bridging table of bridge 2

p1	p2

Learning / Flooding

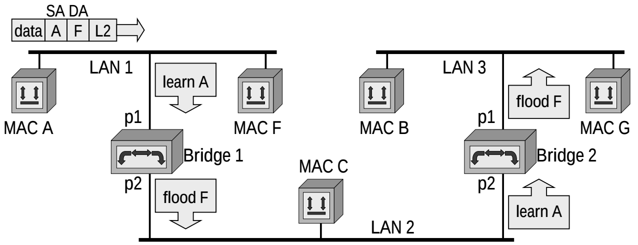


table of Bridge 1

p1	p2
A	

table of Bridge 2

p1	p2
	A

Learning / Filtering

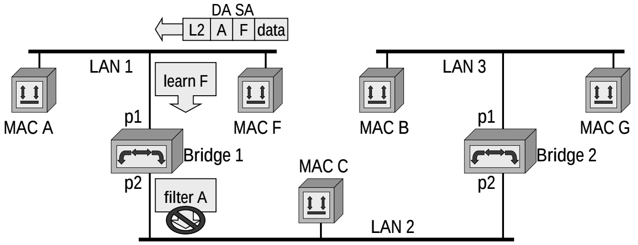
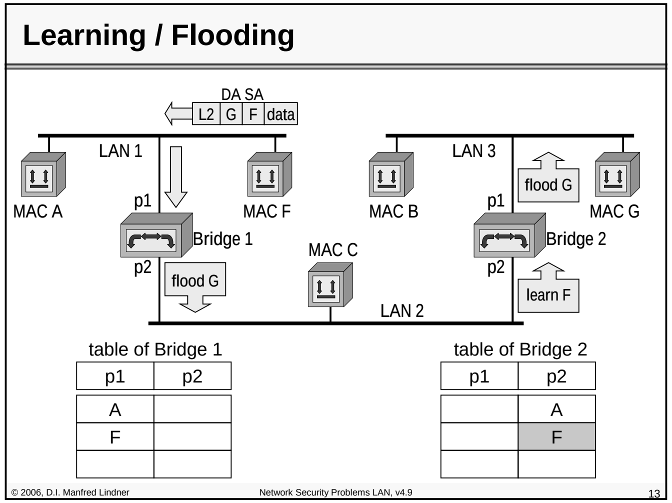


table of Bridge 1

p1	p2
A	
F	

table of Bridge 2

p1	p2
	A



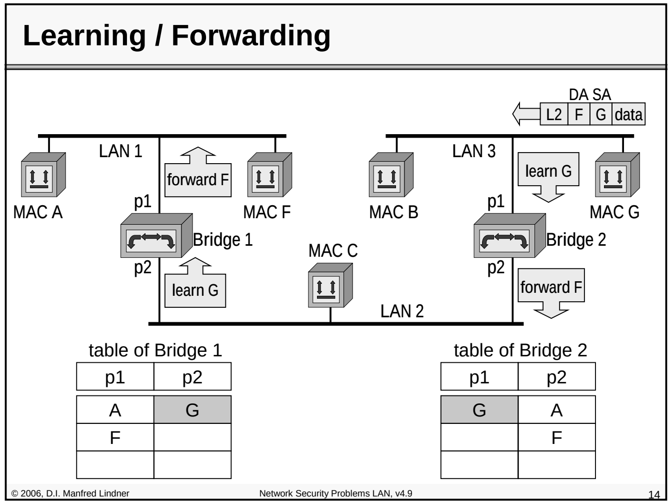
Learning / Flooding

table of Bridge 1

p1	p2
A	
F	

table of Bridge 2

p1	p2
	A
	F



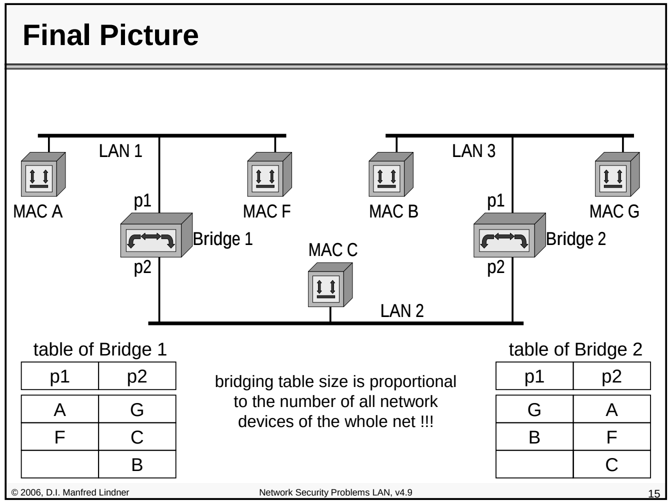
Learning / Forwarding

table of Bridge 1

p1	p2
A	G
F	

table of Bridge 2

p1	p2
G	A
	F



Final Picture

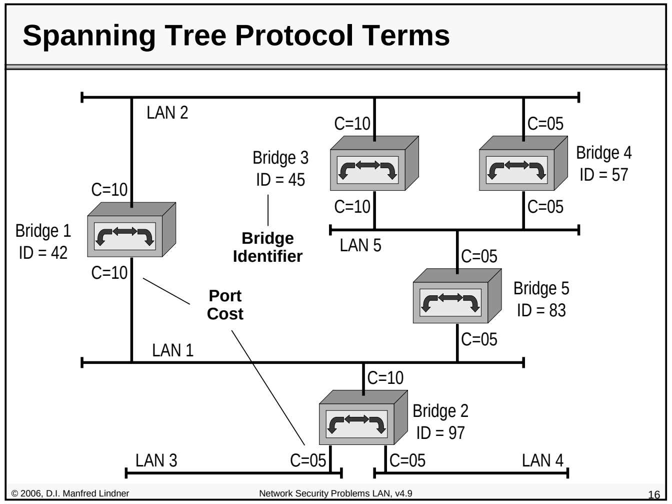
table of Bridge 1

p1	p2
A	G
F	C
	B

bridging table size is proportional to the number of all network devices of the whole net !!!

table of Bridge 2

p1	p2
G	A
B	F
	C



Spanning Tree Protocol Terms

Format of STP Messages - BPDU Format

Prot. ID	Prot. Vers.	BPDU Type	Flags	Root ID	Root Path Costs	Bridge ID	Port ID	Mess. Age	Max Age	Hello Time	Fwd. Delay
2 Byte	1 Byte	1 Byte	1 Byte	8 Byte	4 Byte	8 Byte	2 Byte	2 Byte	2 Byte	2 Byte	2 Byte

BPDU .... Bridge Protocol Data Unit (OSI term for this kind of message)

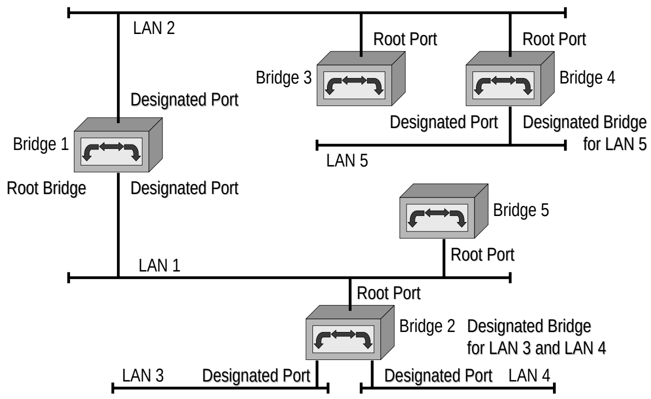
Root ID .... Who seems to be or who is the root bridge (R-ID)?

Root Path Cost .... How far is the root bridge away from me (RPC)?

Bridge ID .... ID of bridge transmitting this BPDU (O-ID)

Port ID .... port over which this BPDU was transmitted (P-ID)

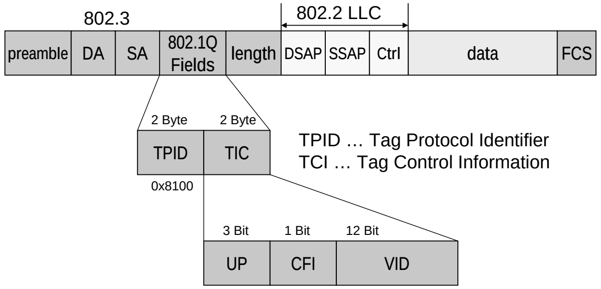
Spanning Tree Applied



Review L2 Network Components

- **VLAN Switch**
  - – Several virtual Ethernet switches in one physical box
  - – Each of them implementing a separate Virtual LAN to corresponding connected LAN user ports (access ports)
    - A separate bridging table per VLAN
  - – Trunk ports used for interconnection of VLAN switches
    - VLAN Tagging (IEEE 802.1Q or Cisco ISL)
    - VLAN management protocols (like Cisco's VTP, DTP)
  - – Sometimes access ports
    - Use VLAN tagging to connect a network station (PC, router, firewall, etc…) to several VLAN's
  - – "Spanning Tree Protocol"
    - One Single STP for all VLAN's (802.1D)
    - Per VLAN STP (Cisco)
    - MIST (802.1w)

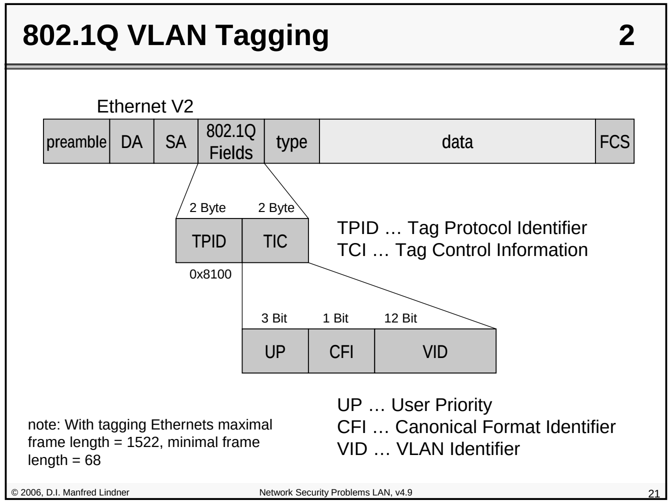
802.1Q VLAN Tagging 1



TPID … Tag Protocol Identifier
TCI … Tag Control Information

UP … User Priority
CFI … Canonical Format Identifier
VID … VLAN Identifier

note: With tagging Ethernets maximal frame length = 1522, minimal frame length = 68



802.1Q VLAN Tagging 2

Ethernet V2

preamble	DA	SA	802.1Q Fields	type	data	FCS

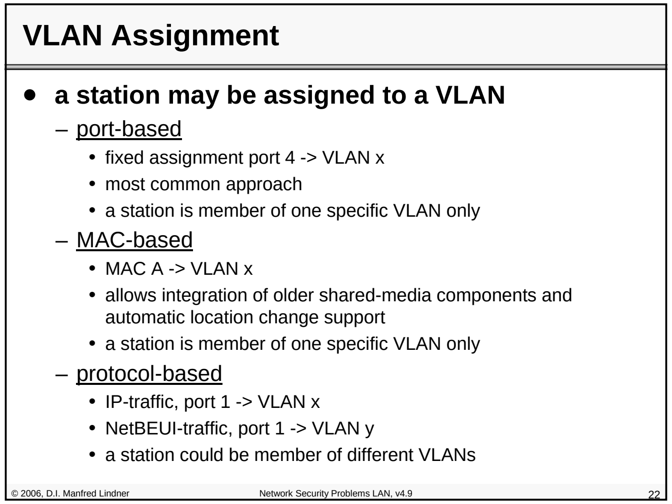
2 Byte	2 Byte
TPID	TIC
0x8100	

TPID … Tag Protocol Identifier
TCI … Tag Control Information

3 Bit	1 Bit	12 Bit
UP	CFI	VID

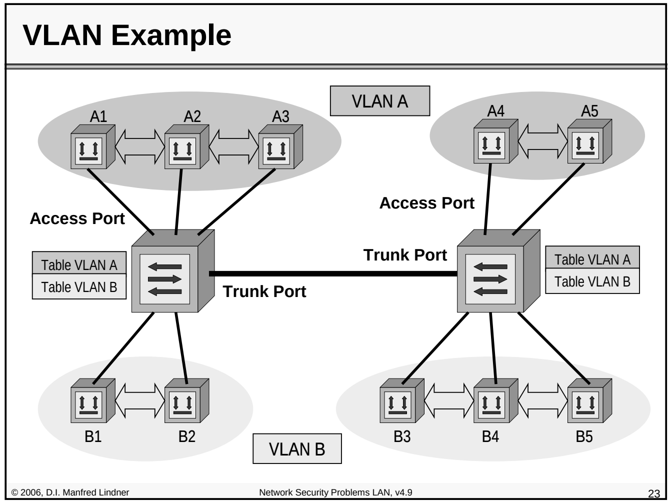
UP … User Priority
CFI … Canonical Format Identifier
VID … VLAN Identifier

note: With tagging Ethernets maximal frame length = 1522, minimal frame length = 68

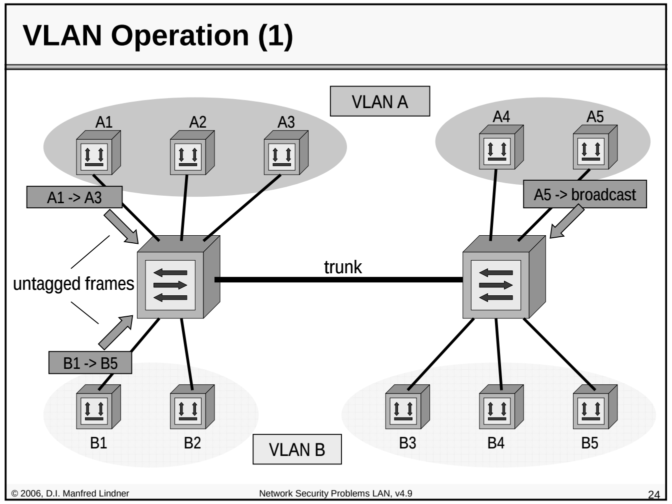


VLAN Assignment

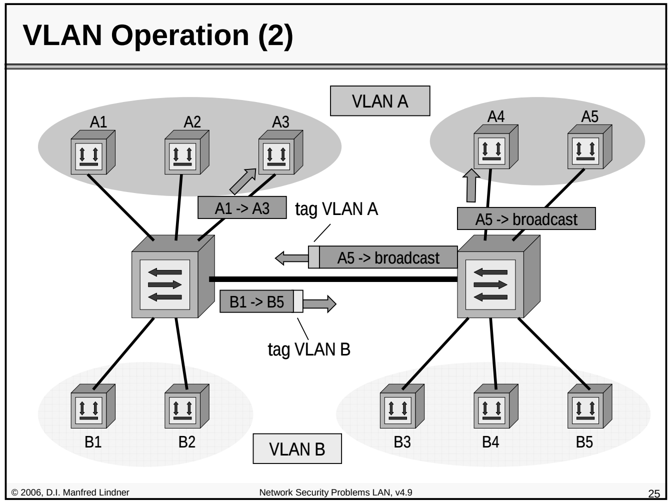
- **a station may be assigned to a VLAN**
  - port-based
    - fixed assignment port 4 -> VLAN x
    - most common approach
    - a station is member of one specific VLAN only
  - MAC-based
    - MAC A -> VLAN x
    - allows integration of older shared-media components and automatic location change support
    - a station is member of one specific VLAN only
  - protocol-based
    - IP-traffic, port 1 -> VLAN x
    - NetBEUI-traffic, port 1 -> VLAN y
    - a station could be member of different VLANs



VLAN Example

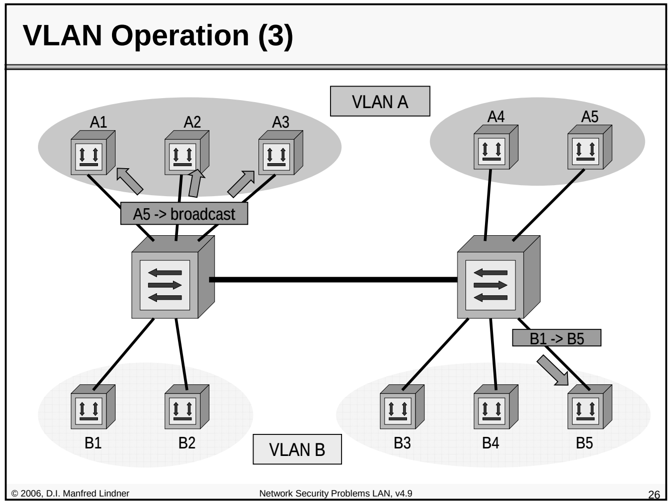


VLAN Operation (1)



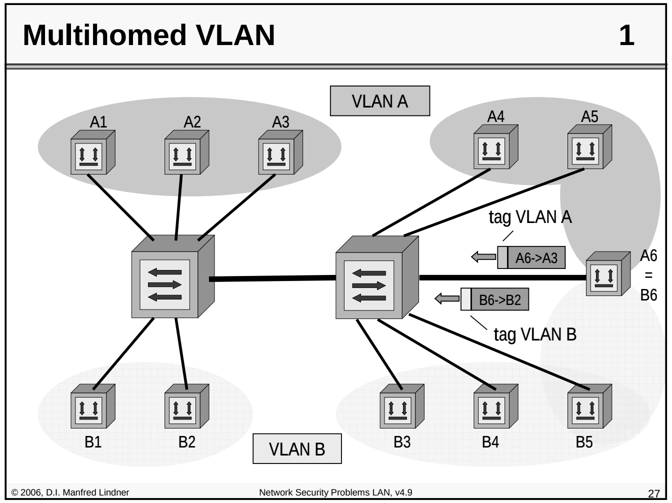
VLAN Operation (2)

© 2006, D.I. Manfred Lindner Network Security Problems LAN, v4.9 25



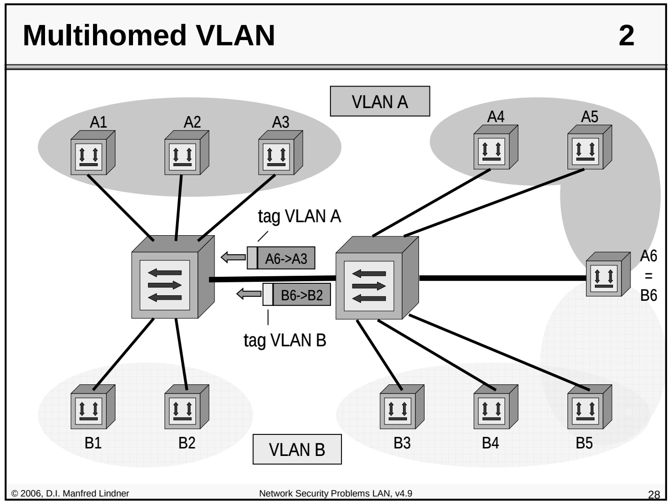
VLAN Operation (3)

© 2006, D.I. Manfred Lindner Network Security Problems LAN, v4.9 26



Multihomed VLAN 1

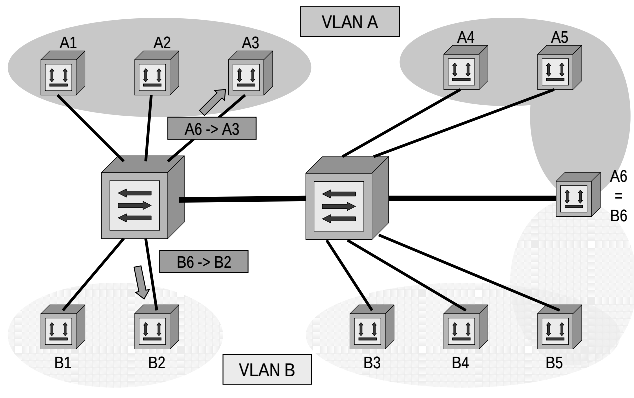
© 2006, D.I. Manfred Lindner Network Security Problems LAN, v4.9 27



Multihomed VLAN 2

© 2006, D.I. Manfred Lindner Network Security Problems LAN, v4.9 28

Multihomed VLAN 3



Agenda

- **L1**
- **L2**
  - Review L2 Components and Functions
  - L2 Attacks
- **L2/L3**
  - Review ARP
  - L2/L3 Attack ARP Spoofing
  - Review DHCP
  - L2/L3/L7 Attack DHCP Spoofing
- **Wireless**
  - Review
  - Attacks

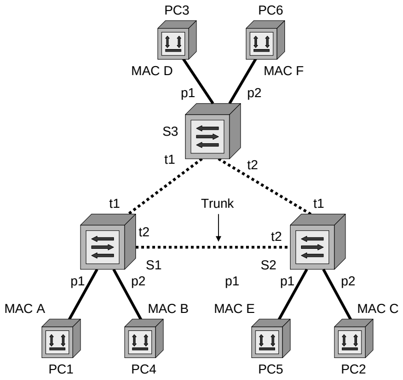
Overview Attacks on L2

- **Network Sniffing**
  - Capturing traffic
- **MAC Flooding**
  - Overloading bridging/switching table
- **MAC Spoofing**
  - Falsifying MAC address
- **STP Spoofing**
  - Disturbing/manipulating BPDU messages
- **VLAN Spoofing**
  - Disturbing/manipulation 802.1Q tagging

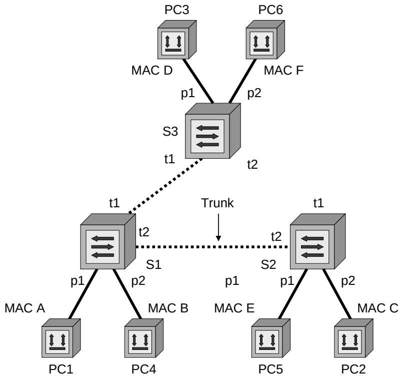
Attacks on LANs (L2) 1

- **Network sniffing (passive attack)**
  - enable “promiscuous mode” on your Ethernet card and you will receive all traffic which appears at your card
  - in a repeater environment or wireless environment you will see every frame carried over the shared media
  - in a bridged/switched environment you will see only Ethernet frames destined to your MAC address and broadcast / multicast frames
    - assumption: bridge has already learned all MAC addresses of the given LAN and hence flooding is not used any longer
  - often part of a “Trojan” software which will sniff on a far remote LAN and will report to the intruder station over a so called covert-channel

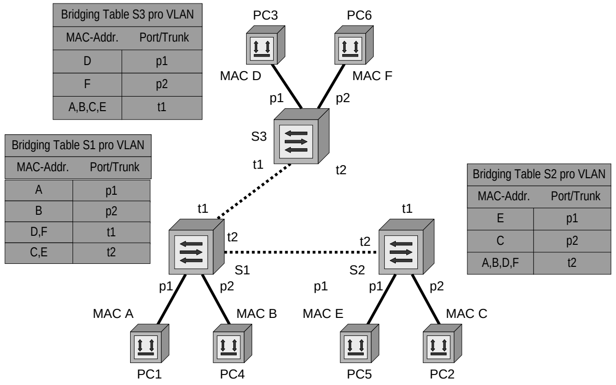
Topologie L2 Switching



Spanning Tree Applied



Bridging/Switching Table (L2)



Bridging Table S3 pro VLAN

MAC-Addr.	Port/Trunk
D	p1
F	p2
A,B,C,E	t1

Bridging Table S1 pro VLAN

MAC-Addr.	Port/Trunk
A	p1
B	p2
D,F	t1
C,E	t2

Bridging Table S2 pro VLAN

MAC-Addr.	Port/Trunk
E	p1
C	p2
A,B,D,F	t2

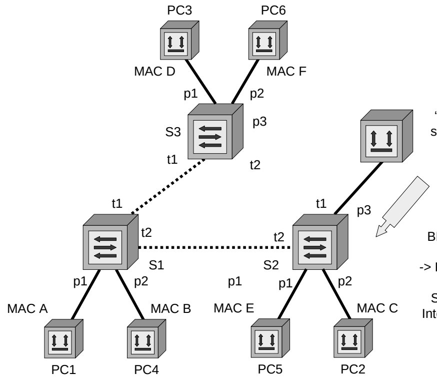
Attacks on LANs (L2) 2

- **MAC flooding (active attack)**
  - – even in a bridged/switched environment you can get all traffic of the given LAN appearing on your card by performing so called “MAC flooding”
  - – get your machine producing a huge number of MAC frames -> every single frame carrying a different MAC address as source address
    - E.g. “macof” utility which comes with “dsniff” suite
  - – bridging / switching table will overrun
  - – will cause the bridge/switch to perform a “Flooding Decision” for every frame received
  - – hence to will see every frame on your LAN

Attacks on LANs (L2) 3

- **MAC address spoofing**
  - BIA address of your Ethernet adapter can be changed
  - so you can impersonate another station
    - either send frames in the name of the impersonated station
    - or receive frames originally destined for this station
- **STP disturbance**
  - An intruder station manipulate BPDU messages to disturb STP operation
    - Kind of DoS (Denial of Service) attack
  - An intruder station with two Ethernet ports manipulate BPDU messages in such a way that it becomes the root bridge
    - All traffic will flow through this machine
    - Kind of "man-in-the-middle" attack

Spanning Tree Disturbance

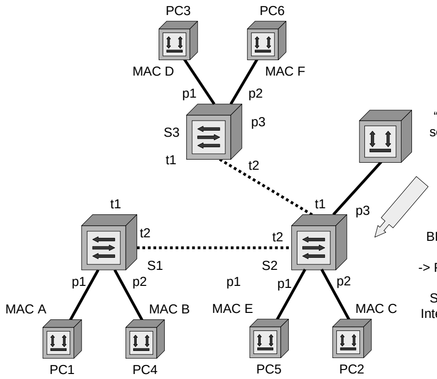


"Rogue" PC acting as switch sends spoofed STP messages in order to disturb STP "Denial of Service" Attack

BPDU with lowest possible value for Bridge ID -> Priority = 0, MAC = 00…01

STP have to be rebuild -> Interruption for a certain time

Spanning Tree Disturbance Result

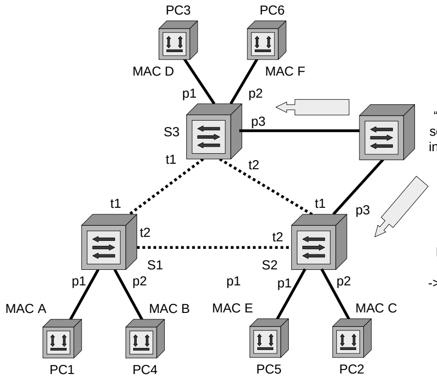


"Rogue" PC acting as switch sends spoofed STP messages in order to disturb STP "Denial of Service" Attack

BPDU with lowest possible value for Bridge ID -> Priority = 0, MAC = 00…01

STP have to be rebuild -> Interruption for a certain time

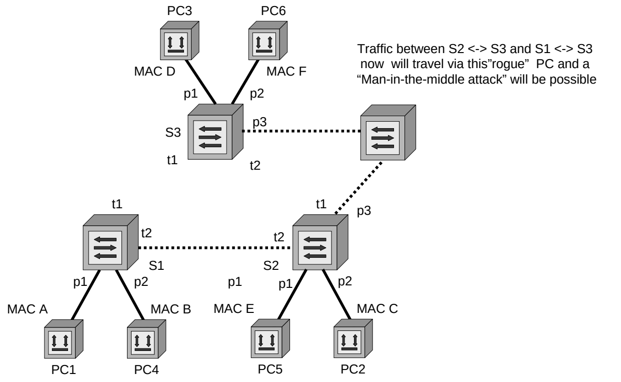
Spanning Tree Spoofing



"Rogue" PC acting as switch sends spoofed STP messages in order to become root bridge

BPDU with lowest possible value for Bridge ID -> Priority = 0, MAC = 00…01

Spanning Tree Spoofing Result

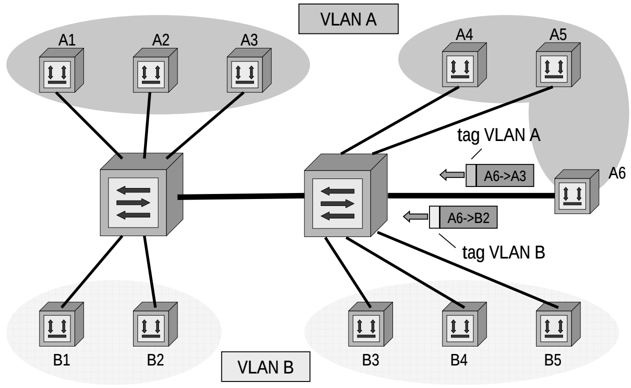


Traffic between S2 <-> S3 and S1 <-> S3 now will travel via this"rogue" PC and a "Man-in-the-middle attack" will be possible

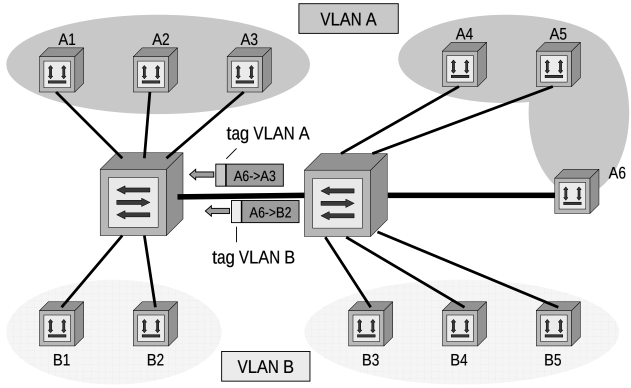
Attacks on LANs (L2) 4

- **VLAN hopping**
  - An intruder station sends VLAN tagged frames instead of normal frames
  - You need a PC Ethernet card which supports 802.1Q VLAN tagging
  - Kind of DoS attack possible
- **VLAN break in**
  - An intruder station makes a switch belief that it is switch
  - Switch may enter trunk mode on that port delivering traffic for all VLAN's on that port
  - Your PC card have to speak the switch special trunking protocols like VTP or ISL
  - Sniffing on all traffic is possible

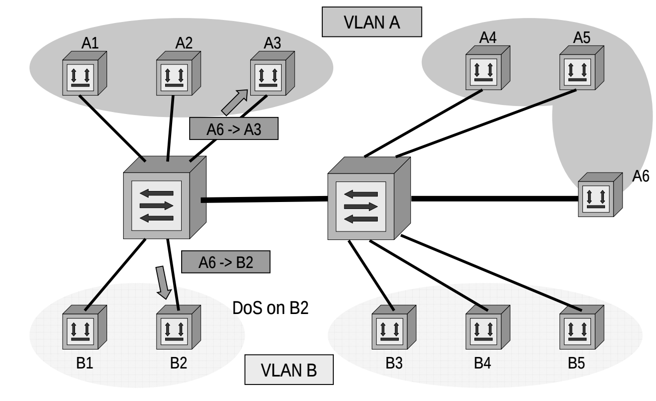
VLAN Hopping 1



VLAN Hopping 2



VLAN Hopping 3



LAN Attacks Mitigation 1

- **Repeater or wireless environment**
  - Solution only possible with cryptographic means
- **Switched environment**
  - Plug and play mode (MAC source address learning, dynamic bridging table)
    - Ethernet switches must be resistant against MAC bridging table flooding on user (access) ports
    - May be achieved by limiting the amount of different MAC addresses seen on a port within a certain time interval (e.g. Cisco’s port security feature)
  - MAC authentication mode (static bridging table)
    - Control who attaches on an access port
    - Maintenance problems may be eased by “freezing” learned MAC addresses
  - MAC filter mode
    - Explicitly define filter rules who is allowed to communicate with whom based on the MAC addresses
    - Hard to maintain, typically achieved by VLAN techniques nowadays

LAN Attacks Mitigation 2

- **Switched environment (cont.)**
  - In all mentioned modes still broadcasts and multicast are seen on all ports
    - Because of the broadcast domain
  - This may provide even in a controlled environment enough information about MAC addresses used by other systems in the switched LAN
  - MAC address can be spoofed
    - Disturbs communication if two systems with same MAC address are active at the same time
      - In case of learning mode, last seen address will overwrite table entry
    - Intruder may takeover role of another machine in times of its absence if authentication is based on MAC address only

LAN Attacks Mitigation 3

- **General rules in today's switched environment:**
  - Restrict access at user ports to authenticated users only
    - MAC address authentication because of MAC address spoofing may be to weak
    - Usage of 802.1x / EAP (Extensible Authentication Protocol) together with a security server like RADIUS or TACACS+ is a possible solution
  - Restrict authorization rights (what is allowed to do) at user (access) ports to that what is really necessary
    - Disable VLAN trunk facilities on access port
    - In case of several VLAN's per access port restrict VLAN-IDs to the intended values
    - Disable (?) handling of STP messages on access port
      - But be careful avoiding the famous broadcast storm by establishing redundant connections between L2 switches

LAN Attacks Mitigation 4

- **General rules in today's switched environment (cont.):**
  - Arrange a management VLAN for remote management of switches totally separated from all other VLAN's
  - Use SNMPv3 instead of SNMPv1 if possible
  - Use SSH instead of Telnet if possible
  - Use HTTPS instead of HTTP if possible

IEEE 802.1x

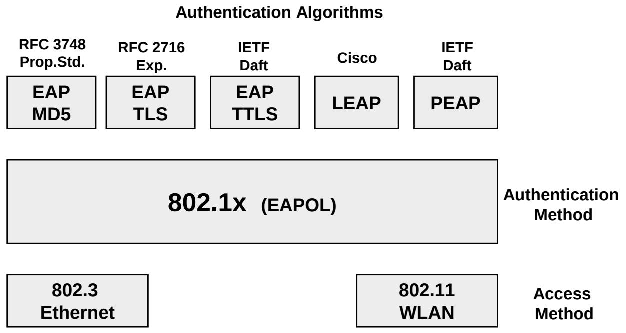
- **IEEE 802.1x**
  - Port-based network access control
  - Authentication and authorization of devices attached to a LAN port with point-to-point connection characteristics
  - Framework for describing the functions and procedures for such an infrastructure (an AAA server like Radius is needed)
  - Defining and coding the transport container of EAP messages
    - EAPOL (EAP encapsulation Over Lan)
      - EAP-Packet
      - EAPOL-Start, EAPOL-Logoff
      - EAPOL-Encapsulated-ASF-Alert
      - EAPOL-Key

IETF EAP

- **EAP (RFC 3748 (RFC 2284, 2484 are obsoleted))**
  - Extensible Authentication Protocol
    - Flexible replacement for PAP and CHAP already known in the RAS area (PPP link)
  - What does flexibility mean?
    - EAP permits the use of a backend authentication server
    - EAP is used to select a specific authentication mechanism
    - Authenticator (e.g. L2 switch or RAS) acting as a pass-through for some or all mechanism
    - Does not require the authenticator to be updated to support each new authentication method
  - Framework for different authentication methods
    - EAP messages and base methods are defined
  - Runs over classical PPP and 802 LANs
    - Using EAP-Packet format of 802.1x in case of 802 LAN

Overview 802.1X / EAP

TLS … Transport Level Security (based on SSL), TTLS … Tunneled TLS
LEAP … Lightweight EA, PEAP …Protected EAP



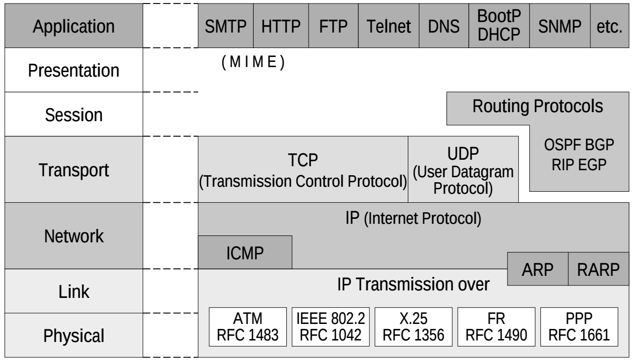
LAN Attacks Mitigation 5

- **How detect a “Sniffer”?**
  - How to detect that an Ethernet card is in promiscuous mode?
  - If performed on an stand-alone system theoretically impossible
  - But in most cases “sniffing” performed on normal machines as add-on to normal IP stack
  - For details see
    - Robert Graham's famous Sniffing (network wiretap, sniffer) FAQ
    - → http://www.secinf.net/misc/Sniffing_network_wiretap_sniffer_FAQ_.html
    - Daiji Sanai’s article: “Detection of promiscuous nodes using ARP”
    - → http://www.securityfriday.com/promiscuous_detection_01.pdf

Agenda

- **L1**
- **L2**
  - Review L2 Components and Functions
  - L2 Attacks
- **L2/L3**
  - Review ARP
  - L2/L3 Attack ARP Spoofing
  - Review DHCP
  - L2/L3/L7 Attack DHCP Spoofing
- **Wireless**
  - Review
  - Attacks

TCP/IP Protocol Suite



ARP Request/Reply Format

Hardware		Protocol (IP = 0x0800)	
hln	pln	Operation	
Source Hardware Address (byte 0 - 3)			
Source HW Addr. (byte 4 - 5)		Source IP Addr. (byte 0 - 1)	
Source IP Addr. (byte 2 - 3)		Dest. HW Addr. (byte 0 - 1)*	
Destination Hardware Address (byte 2 - 5)*			
Destination IP Address (byte 0 - 3)			

*) Destination hardware address is left empty (hex FF FF FF FF FF FF) for ARP request.

ARP Request/Reply Fields

- **Hardware**
  - Defines the type of network hardware, e.g.:

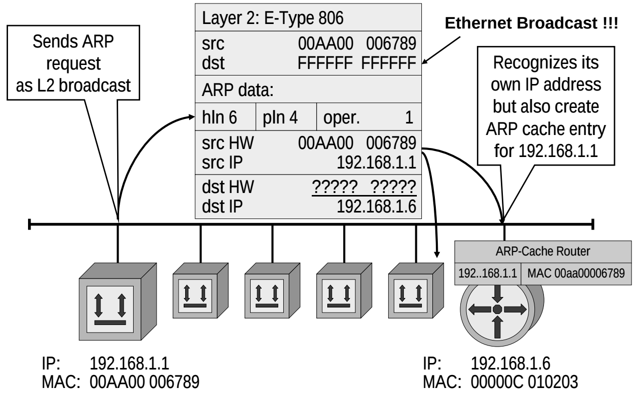
1	Ethernet DIX
6	802.x-LAN
7	ARCNET
11	LocalTalk

- **Protocol**
  - Selects the layer 3 protocol (uses the values which are defined for the Ethernet type field, e.g. 0x800 for IP)
- **hln**
  - Length of hardware address in bytes

ARP Request/Reply Fields

- **pln**
  - Length of layer 3 address in bytes
- **Operation**
  - 1 .... ARP Request
  - 2 .... ARP Reply
  - 3 .... RARP Request
  - 4 .... RARP Reply
- **Addresses**
  - Hardware addresses: MAC addresses (src. and dest.)
  - IP addresses: layer 3 addresses (src. and dest.)
- **ARP request and replies are never forwarded by routers (only LAN broadcast used)**

ARP Request in Detail



Layer 2: E-Type 806

src 00AA00 006789

dst FFFFFF FFFFFF

ARP data:

hln 6 | pln 4 | oper. 1

src HW 00AA00 006789

src IP 192.168.1.1

dst HW ????? ?????

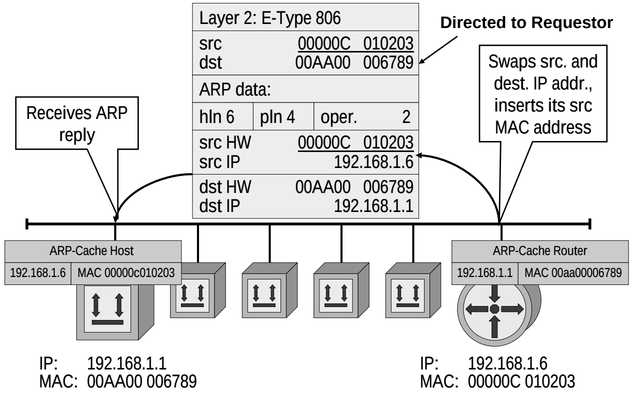
dst IP 192.168.1.6

Ethernet Broadcast !!!

Sends ARP request as L2 broadcast

Recognizes its own IP address but also create ARP cache entry for 192.168.1.1

ARP Reply in Detail



Layer 2: E-Type 806

src 00000C 010203

dst 00AA00 006789

ARP data:

hln 6 | pln 4 | oper. 2

src HW 00000C 010203

src IP 192.168.1.6

dst HW 00AA00 006789

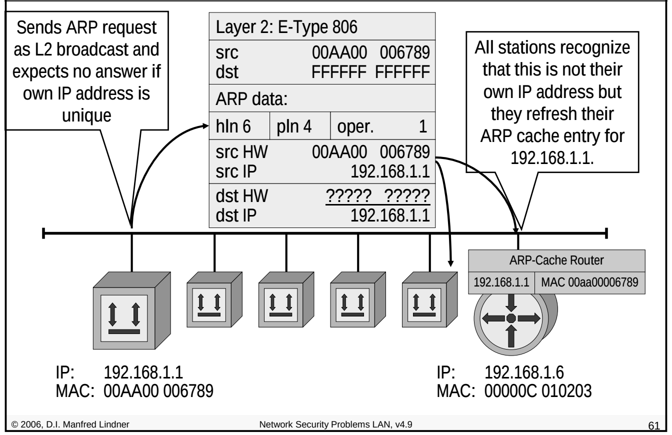
dst IP 192.168.1.1

Directed to Requestor

Receives ARP reply

Swaps src. and dest. IP addr., inserts its src MAC address

Gratuitous ARP for Duplicate Address Check and ARP Cache Refresh



Sends ARP request as L2 broadcast and expects no answer if own IP address is unique

Layer 2: E-Type 806		
src dst	00AA00 006789 FFFFFF FFFFFF	
ARP data:		
hln 6	pln 4	oper. 1
src HW src IP	00AA00 006789 192.168.1.1	
dst HW dst IP	????? ????? 192.168.1.1	

All stations recognize that this is not their own IP address but they refresh their ARP cache entry for 192.168.1.1.

ARP-Cache Router	
192.168.1.1	MAC 00aa00006789

IP: 192.168.1.1
MAC: 00AA00 006789

IP: 192.168.1.6
MAC: 00000C 010203

Agenda

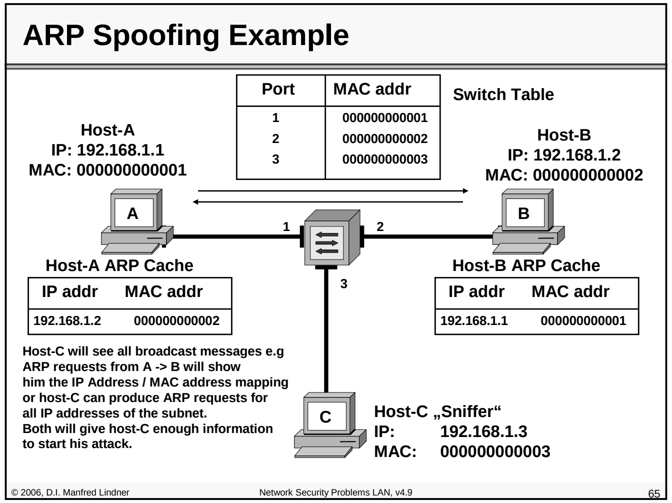
- **L1**
- **L2**
  - Review L2 Components and Functions
  - L2 Attacks
- **L2/L3**
  - Review ARP
  - L2/L3 Attack ARP Spoofing
  - Review DHCP
  - L2/L3/L7 Attack DHCP Spoofing
- **Wireless**
  - Review
  - Attacks

Attacks on L2/L3 (ARP, IP)

- **ARP Spoofing**
  - Falsify MAC address
  - Man-in-the-middle attack

ARP Spoofing

- **Aka ARP Poisoning**
  - well know weakness in TCP/IP is the ARP (Address Resolution Protocol
    - no authentication, stateless
  - ARP Spoofing:
    - Control the ARP Cache of foreign machines A and B in such a way (faked ARP entries) that all IP packets from A to B and vice versa are redirected to the MAC address of an intruder machine
  - a hacker with the right tools (e.g. „Cain and Able“) can exploit ARP and take control of the LAN/WLAN
  - see http://www.oxid.it/topics.html for details
  - if one of the faked machines is the default gateway
    - all traffic of a IP subnet to the Internet and vice versa could be redirected to the intruder



ARP Spoofing Example

Switch Table

Port	MAC addr
1	000000000001
2	000000000002
3	000000000003

Host-A ARP Cache

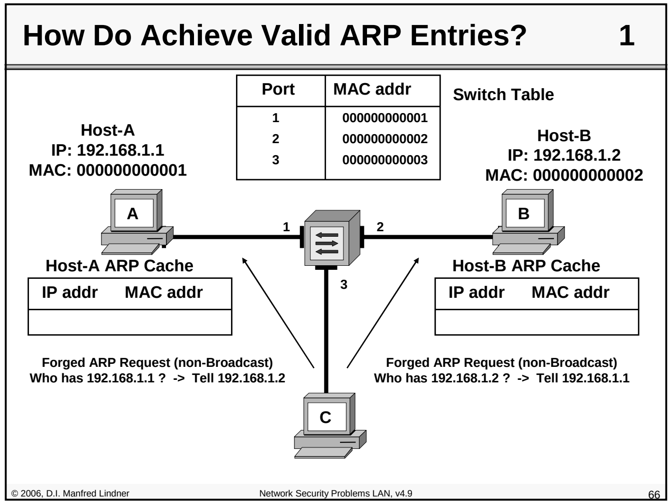
IP addr	MAC addr
192.168.1.2	000000000002

Host-B ARP Cache

IP addr	MAC addr
192.168.1.1	000000000001

Host-C will see all broadcast messages e.g ARP requests from A -> B will show him the IP Address / MAC address mapping or host-C can produce ARP requests for all IP addresses of the subnet. Both will give host-C enough information to start his attack.

© 2006, D.I. Manfred Lindner Network Security Problems LAN, v4.9 65



How Do Achieve Valid ARP Entries? 1

Switch Table

Port	MAC addr
1	000000000001
2	000000000002
3	000000000003

Host-A ARP Cache

IP addr	MAC addr

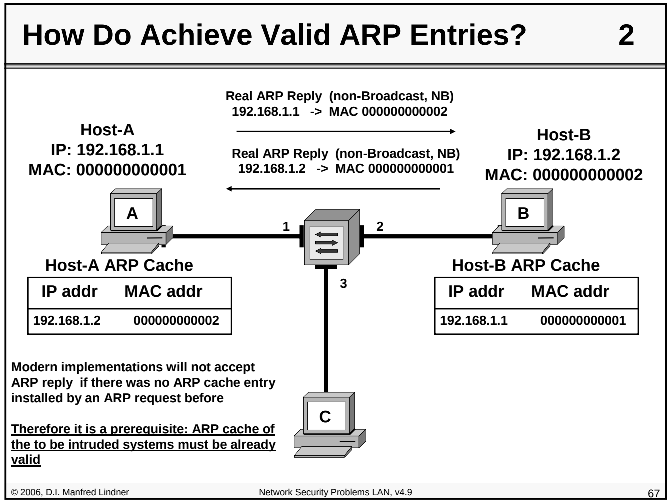
Host-B ARP Cache

IP addr	MAC addr

Forged ARP Request (non-Broadcast)
Who has 192.168.1.1 ? -> Tell 192.168.1.2

Forged ARP Request (non-Broadcast)
Who has 192.168.1.2 ? -> Tell 192.168.1.1

© 2006, D.I. Manfred Lindner Network Security Problems LAN, v4.9 66



How Do Achieve Valid ARP Entries? 2

Real ARP Reply (non-Broadcast, NB)
192.168.1.1 -> MAC 000000000002

Real ARP Reply (non-Broadcast, NB)
192.168.1.2 -> MAC 000000000001

Host-A ARP Cache

IP addr	MAC addr
192.168.1.2	000000000002

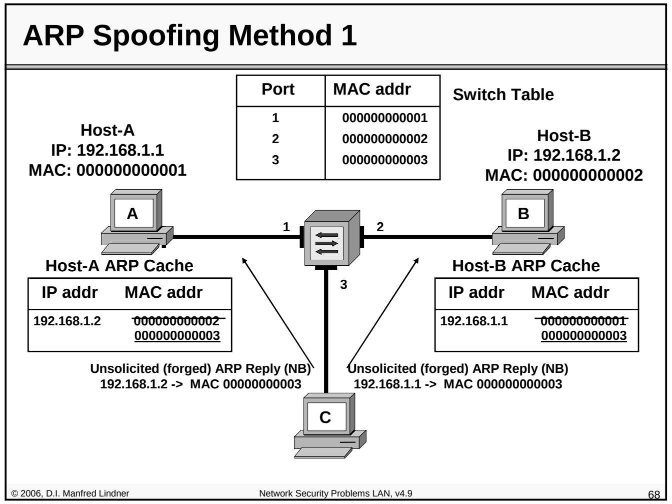
Host-B ARP Cache

IP addr	MAC addr
192.168.1.1	000000000001

Modern implementations will not accept ARP reply if there was no ARP cache entry installed by an ARP request before

Therefore it is a prerequisite: ARP cache of the to be intruded systems must be already valid

© 2006, D.I. Manfred Lindner Network Security Problems LAN, v4.9 67



ARP Spoofing Method 1

Switch Table

Port	MAC addr
1	000000000001
2	000000000002
3	000000000003

Host-A ARP Cache

IP addr	MAC addr
192.168.1.2	~~000000000002~~ 000000000003

Host-B ARP Cache

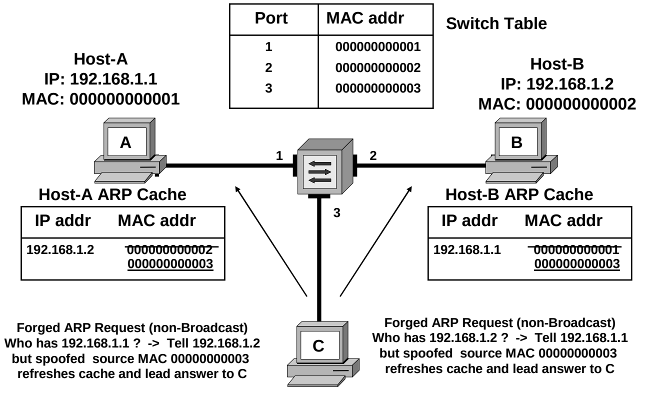
IP addr	MAC addr
192.168.1.1	~~000000000001~~ 000000000003

Unsolicited (forged) ARP Reply (NB)
192.168.1.2 -> MAC 00000000003

Unsolicited (forged) ARP Reply (NB)
192.168.1.1 -> MAC 000000000003

© 2006, D.I. Manfred Lindner Network Security Problems LAN, v4.9 68

ARP Spoofing Method 2



Switch Table

Port	MAC addr
1	000000000001
2	000000000002
3	000000000003

Host-A
IP: 192.168.1.1
MAC: 000000000001

Host-B
IP: 192.168.1.2
MAC: 000000000002

Host-A ARP Cache

IP addr	MAC addr
192.168.1.2	~~000000000002~~ 000000000003

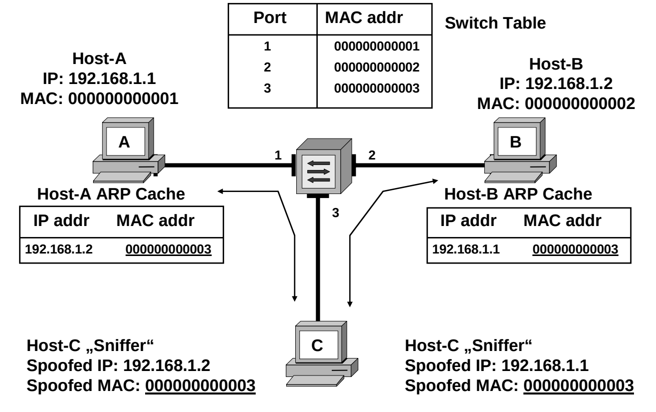
Host-B ARP Cache

IP addr	MAC addr
192.168.1.1	~~000000000001~~ 000000000003

Forged ARP Request (non-Broadcast)
Who has 192.168.1.1 ? -> Tell 192.168.1.2
but spoofed source MAC 00000000003
refreshes cache and lead answer to C

Forged ARP Request (non-Broadcast)
Who has 192.168.1.2 ? -> Tell 192.168.1.1
but spoofed source MAC 00000000003
refreshes cache and lead answer to C

ARP Spoofing in Action



Switch Table

Port	MAC addr
1	000000000001
2	000000000002
3	000000000003

Host-A
IP: 192.168.1.1
MAC: 000000000001

Host-B
IP: 192.168.1.2
MAC: 000000000002

Host-A ARP Cache

IP addr	MAC addr
192.168.1.2	000000000003

Host-B ARP Cache

IP addr	MAC addr
192.168.1.1	000000000003

Host-C „Sniffer"
Spoofed IP: 192.168.1.2
Spoofed MAC: 000000000003

Host-C „Sniffer"
Spoofed IP: 192.168.1.1
Spoofed MAC: 000000000003

Hijacking L2

- **ARP Spoofing together with sniffing and appropriate software running on the intruders machine**
  - Allows to hijack the passing traffic
  - Every packet can be manipulated by the intruder
  - Classical "Man-in-the-middle" attack in a LAN environment
- **There are some means to prevent that**
  - See following slides
- **But the real solution for security**
  - Is end-system to end-system security
  - Crypto-graphical "signatures" for authentication and message integrity of packets

ARP Spoofing Mitigation

- **Allow only static ARP Cache entries in end-systems**
  - Not a practicable solution
- **Install special programs on end-systems**
  - E.g. ArpWatch und XArp
- **Solve the problem at the switch, not at every individual end-system**
  - E.g Cisco's
    "Dynamic ARP Inspection" (DAI) together with **DHCP snooping**
  - On switches ports are categorized as trusted (where the real DHCP server resides) and non-trusted (where the end users reside)
  - DHCP bindings (IP address –> MAC address on which port) are stored in the switch
    - On non-trusted ports certain DHCP messages are not accepted (DHCP ACK, DCP NAK, DHCP Offer)
  - Forged ARP replies are filtered by the switch based on the information of DHCP bindings

Agenda

- **L1**
- **L2**
  - – Review L2 Components and Functions
  - – L2 Attacks
- **L2/L3**
  - – Review ARP
  - – L2/L3 Attack ARP Spoofing
  - – Review DHCP
  - – L2/L3/L7 Attack DHCP Spoofing
- **Wireless**
  - – Review
  - – Attacks

DHCP (Dynamic Host Configuration Protocol)

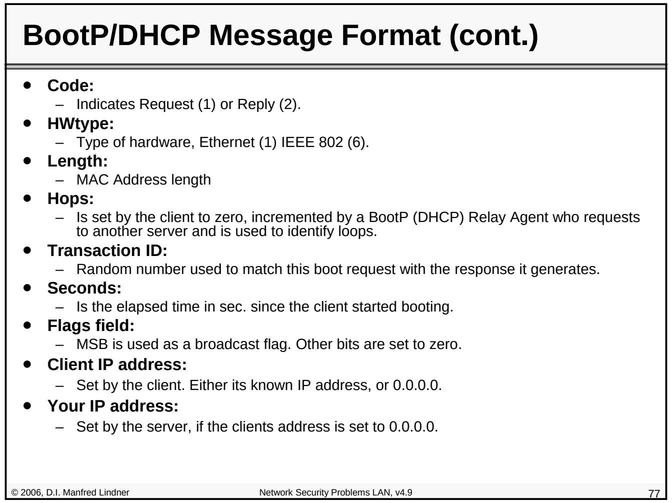
- **DHCP (RFC 2131, 3396) build on two components:**
  - – Protocol to deliver host specific configurations from a server to its client
  - – Mechanism to allocate temporary or permanent host addresses
- **Temporary address allocation**
  - – DHCP server receives a request from a DHCP client and picks out an IP address from a configurable address pool and offers this address to the client
  - – the client can use this leased address for a period of time
  - – after the end of this lease, the address must again be requested by the client or is returned to the address pool

DHCP Configurable Parameters

- **A DHCP client can asks for:**
  - IP address
  - Subnet Mask
  - DNS Server, NetBIOS-Name Server
  - default TTL, Source Routing Option, MTU
  - max. Fragment Size, Broadcast Address
  - List of Default Gateways + Preferences, Static Routes
  - ARP Cache Timeout, TCP Keepalives
  - Ethernet Encapsulation
  - Path MTU Discovery (RFC1191)
  - Router Discovery (RFC 1256)
- **DHCP is based on BootP using the options field (opt. 53) of the BootP header**
  - – port 67 UDP (BootP Server) and port 68 (BootP Client).

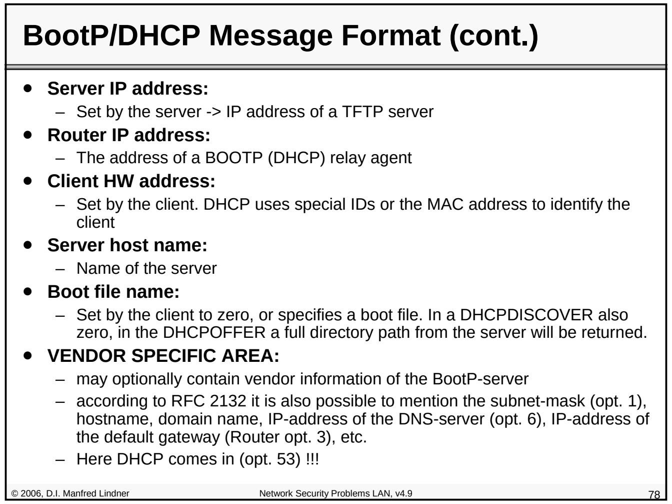
BootP/DHCP Message Format

code	**HWtype**	**length**	**hops**
Transaction ID			
seconds		**Flags field**	
Client IP address			
Your IP address			
Server IP address			
Router IP address (DHCP Relay Agent Address !!!)			
Client HW Address 64 byte			
Server host name 64 byte			
Boot file name 128 byte			
Options variable length (at least 312 byte) (here are the DHCP messages !!!)			



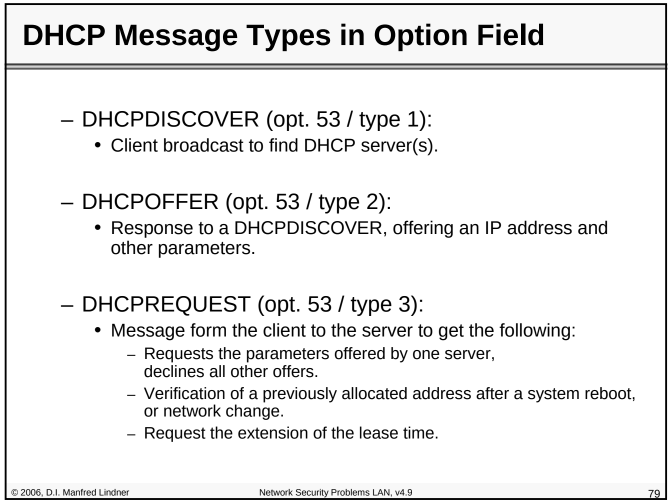
BootP/DHCP Message Format (cont.)

- **Code:**
  - Indicates Request (1) or Reply (2).
- **HWtype:**
  - Type of hardware, Ethernet (1) IEEE 802 (6).
- **Length:**
  - MAC Address length
- **Hops:**
  - Is set by the client to zero, incremented by a BootP (DHCP) Relay Agent who requests to another server and is used to identify loops.
- **Transaction ID:**
  - Random number used to match this boot request with the response it generates.
- **Seconds:**
  - Is the elapsed time in sec. since the client started booting.
- **Flags field:**
  - MSB is used as a broadcast flag. Other bits are set to zero.
- **Client IP address:**
  - Set by the client. Either its known IP address, or 0.0.0.0.
- **Your IP address:**
  - Set by the server, if the clients address is set to 0.0.0.0.



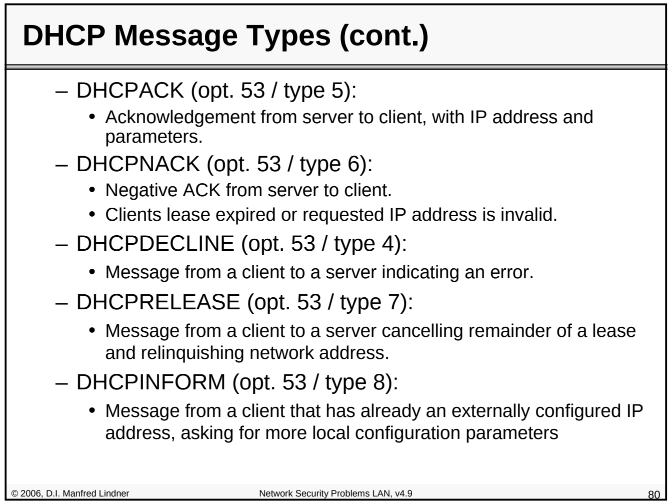
BootP/DHCP Message Format (cont.)

- **Server IP address:**
  - Set by the server -> IP address of a TFTP server
- **Router IP address:**
  - The address of a BOOTP (DHCP) relay agent
- **Client HW address:**
  - Set by the client. DHCP uses special IDs or the MAC address to identify the client
- **Server host name:**
  - Name of the server
- **Boot file name:**
  - Set by the client to zero, or specifies a boot file. In a DHCPDISCOVER also zero, in the DHCPOFFER a full directory path from the server will be returned.
- **VENDOR SPECIFIC AREA:**
  - may optionally contain vendor information of the BootP-server
  - according to RFC 2132 it is also possible to mention the subnet-mask (opt. 1), hostname, domain name, IP-address of the DNS-server (opt. 6), IP-address of the default gateway (Router opt. 3), etc.
  - Here DHCP comes in (opt. 53) !!!



DHCP Message Types in Option Field

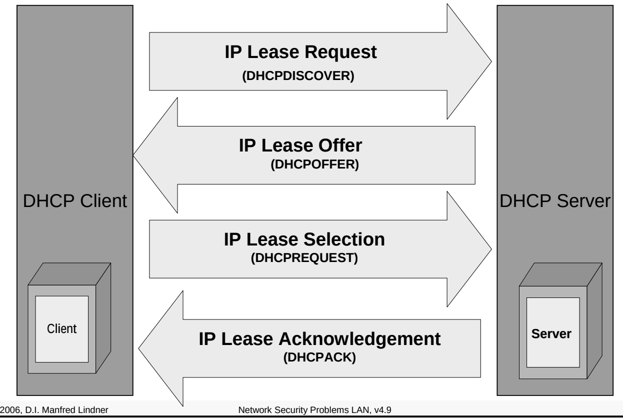
- DHCPDISCOVER (opt. 53 / type 1):
  - Client broadcast to find DHCP server(s).
- DHCPOFFER (opt. 53 / type 2):
  - Response to a DHCPDISCOVER, offering an IP address and other parameters.
- DHCPREQUEST (opt. 53 / type 3):
  - Message form the client to the server to get the following:
    - Requests the parameters offered by one server, declines all other offers.
    - Verification of a previously allocated address after a system reboot, or network change.
    - Request the extension of the lease time.



DHCP Message Types (cont.)

- DHCPACK (opt. 53 / type 5):
  - Acknowledgement from server to client, with IP address and parameters.
- DHCPNACK (opt. 53 / type 6):
  - Negative ACK from server to client.
  - Clients lease expired or requested IP address is invalid.
- DHCPDECLINE (opt. 53 / type 4):
  - Message from a client to a server indicating an error.
- DHCPRELEASE (opt. 53 / type 7):
  - Message from a client to a server cancelling remainder of a lease and relinquishing network address.
- DHCPINFORM (opt. 53 / type 8):
  - Message from a client that has already an externally configured IP address, asking for more local configuration parameters

DHCP Operation



Agenda

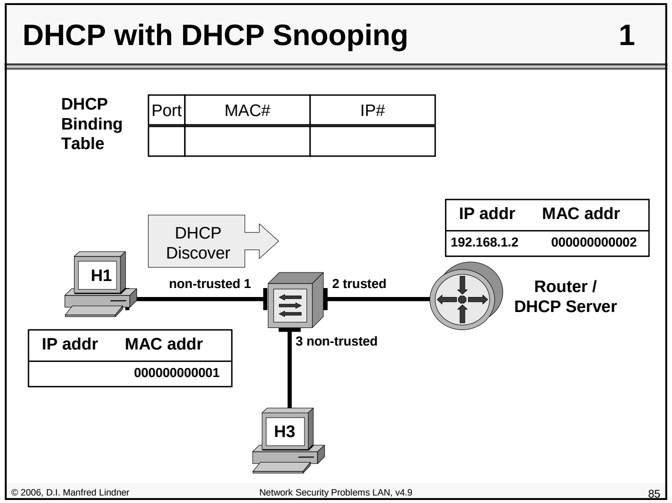
- **L1**
- **L2**
  - Review L2 Components and Functions
  - L2 Attacks
- **<u>L2/L3</u>**
  - Review ARP
  - L2/L3 Attack ARP Spoofing
  - Review DHCP
  - <u>L2/L3/L7 Attack DHCP Spoofing</u>
- **Wireless**
  - Review
  - Attacks

Attacks on L2/L3/L7

- **DHCP Spoofing**
  - Man-in-the-middle attack
  - Falsify Default Gateway IP Address (L3)
  - Falsify DNS Server IP Address (L7)
- **DHCP Starvation**
  - Denial of Service Attack
  - Paralyze real DHCP server by exhausting IP address pool with spoofed MAC addresses in order to install a (rogue) DHCP server of the intruder

DHCP Spoofing / Starvation Mitigation

- **DHCP snooping against DHCP spoofing**
  - Cisco solution
  - On switches ports are categorized as trusted (where the real DHCP server resides) and non-trusted (where the end users reside)
  - On non-trusted ports certain DHCP messages are not accepted (DHCP ACK, DCP NACK, DHCP Offer)
  - Forged DHCP replies are filtered by the switch
- **MAC flooding prevention and/or MAC authentication against DHCP starvation**
  - E.g. Cisco’s “Port Security” feature



DHCP with DHCP Snooping 1

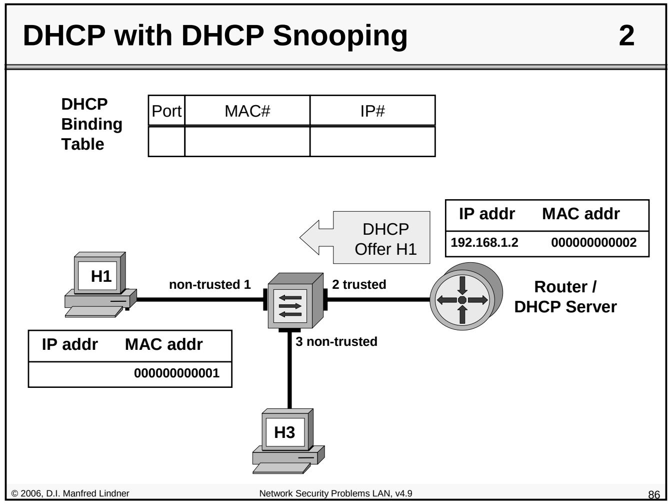
DHCP Binding Table

Port	MAC#	IP#

IP addr	MAC addr
192.168.1.2	000000000002

IP addr	MAC addr
	000000000001

© 2006, D.I. Manfred Lindner Network Security Problems LAN, v4.9 85



DHCP with DHCP Snooping 2

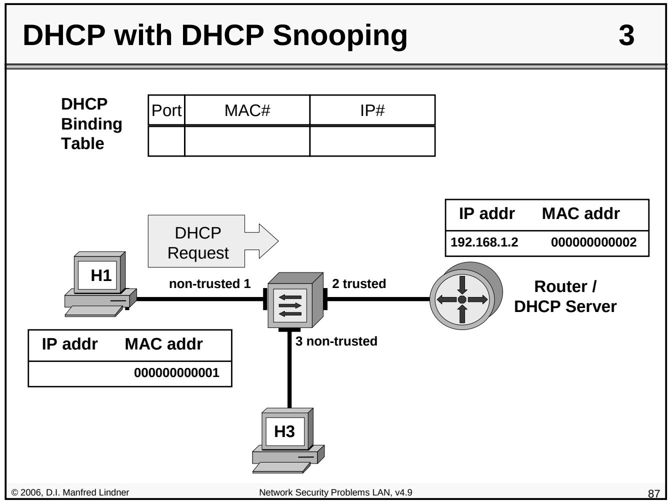
DHCP Binding Table

Port	MAC#	IP#

IP addr	MAC addr
192.168.1.2	000000000002

IP addr	MAC addr
	000000000001

© 2006, D.I. Manfred Lindner Network Security Problems LAN, v4.9 86



DHCP with DHCP Snooping 3

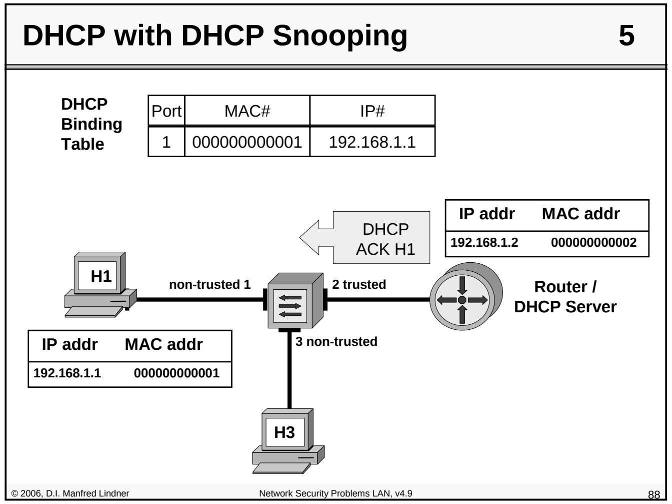
DHCP Binding Table

Port	MAC#	IP#

IP addr	MAC addr
192.168.1.2	000000000002

IP addr	MAC addr
	000000000001

© 2006, D.I. Manfred Lindner Network Security Problems LAN, v4.9 87



DHCP with DHCP Snooping 5

DHCP Binding Table

Port	MAC#	IP#
1	000000000001	192.168.1.1

IP addr	MAC addr
192.168.1.2	000000000002

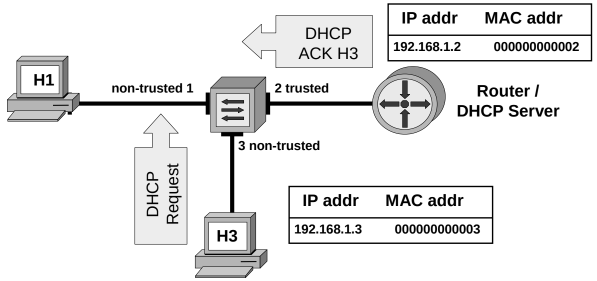
IP addr	MAC addr
192.168.1.1	000000000001

© 2006, D.I. Manfred Lindner Network Security Problems LAN, v4.9 88

DHCP with DHCP Snooping 6

DHCP Binding Table

Port	MAC#	IP#
1	000000000001	192.168.1.1
3	000000000003	192.168.1.3



IP addr	MAC addr
192.168.1.2	000000000002

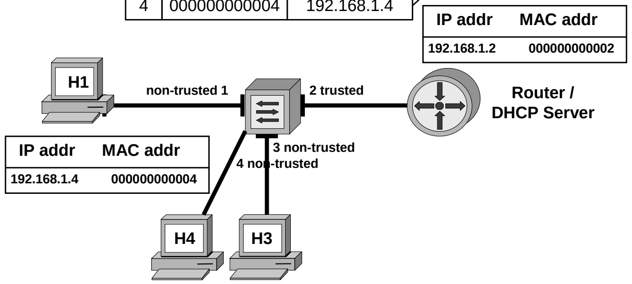
IP addr	MAC addr
192.168.1.3	000000000003

Static Entry with DHCP Snooping 7

DHCP Binding Table

Port	MAC#	IP#
1	000000000001	192.168.1.1
3	000000000003	192.168.1.3
4	000000000004	192.168.1.4

Static entry for non-DHCP clients possible



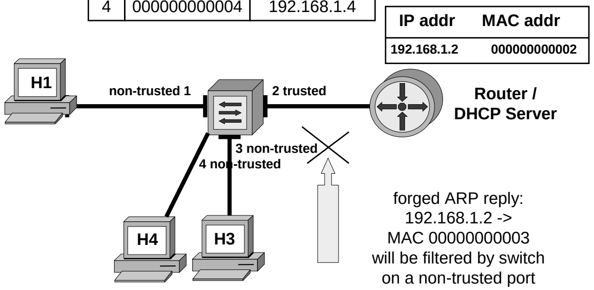
IP addr	MAC addr
192.168.1.2	000000000002

IP addr	MAC addr
192.168.1.4	000000000004

ARP Spoofing Mitigation with Dynamic ARP Inspection (DAI)

DHCP Binding Table

Port	MAC#	IP#
1	000000000001	192.168.1.1
3	000000000003	192.168.1.3
4	000000000004	192.168.1.4



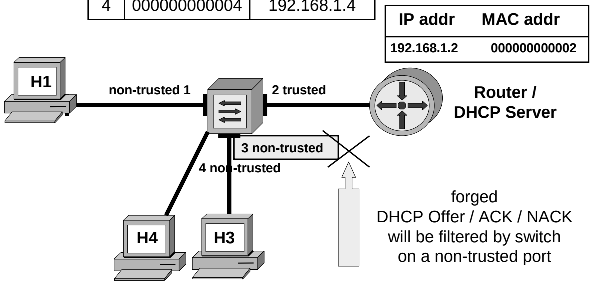
IP addr	MAC addr
192.168.1.2	000000000002

forged ARP reply:
192.168.1.2 ->
MAC 00000000003
will be filtered by switch
on a non-trusted port

DHCP Spoofing Mitigation

DHCP Binding Table

Port	MAC#	IP#
1	000000000001	192.168.1.1
3	000000000003	192.168.1.3
4	000000000004	192.168.1.4



IP addr	MAC addr
192.168.1.2	000000000002

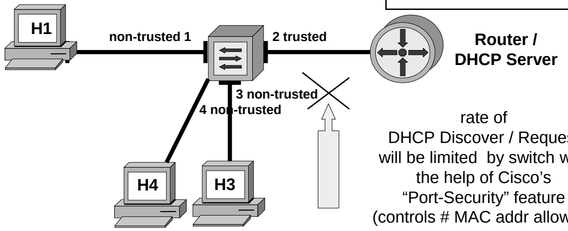
forged
DHCP Offer / ACK / NACK
will be filtered by switch
on a non-trusted port

DHCP Starvation Mitigation

DHCP Binding Table

Port	MAC#	IP#
1	000000000001	192.168.1.1
3	000000000003	192.168.1.3
4	000000000004	192.168.1.4

IP addr	MAC addr
192.168.1.2	000000000002



rate of DHCP Discover / Request will be limited by switch with the help of Cisco's "Port-Security" feature (controls # MAC addr allowed)

Agenda

- **L1**
- **L2**
  - Review L2 Components and Functions
  - L2 Attacks
- **L2/L3**
  - Review ARP
  - L2/L3 Attack ARP Spoofing
  - Review DHCP
  - L2/L3/L7 Attack DHCP Spoofing
- **Wireless**
  - Review
  - Attacks

Wireless LAN

- **Again a shared media for a lot of stations**
  - located around a WLAN access point
    - Infrastructure Mode
  - sharing done by combination of TDM (CSMA/CA) and FDM
    - TDM … Time Division Multiplexing
    - FDM … Frequency Division Multiplexing
    - CA … Collision Avoidance
- **Everybody equipped with the proper equipment (WLAN card)**
  - can listen to the traffic going on
  - can sent traffic to the access point

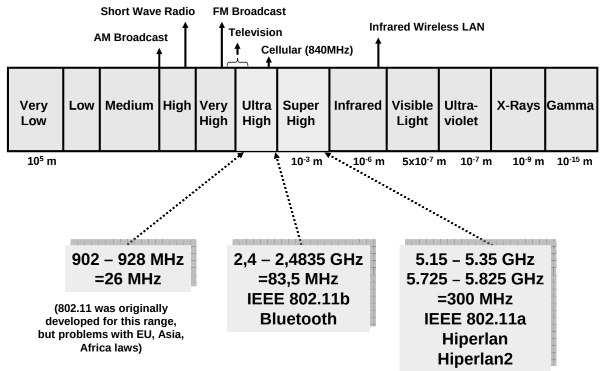
IEEE 802.11 Standard

- **Another IEEE working group**
- **Most successful WLAN standard**
  - Easy and robust wireless LAN
  - Infrared and radio transmission
  - Worldwide use (2,4 GHz)
  - "WIFI-Standard"
  - 1-54 Mbit/s
- **Infrastructure and Ad-hoc design**

IEEE Working Groups

802.1 Higher Layer LAN Protocols
802.2 Logical Link Control
802.3 Ethernet
802.4 Token Bus
802.5 Token Ring
802.6 Metropolitan Area Network
802.7 Broadband TAG
802.8 Fiber Optic TAG
802.9 Isochronous LAN
802.10 Security
802.11 Wireless LAN
802.12 Demand Priority
802.13 Not Used
802.14 Cable Modem
802.15 Wireless Personal Area Network
802.16 Broadband Wireless Access
802.17 Resilient Packet Ring

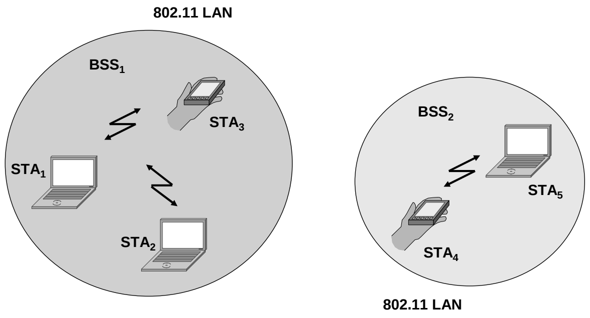
License Free ISM Band



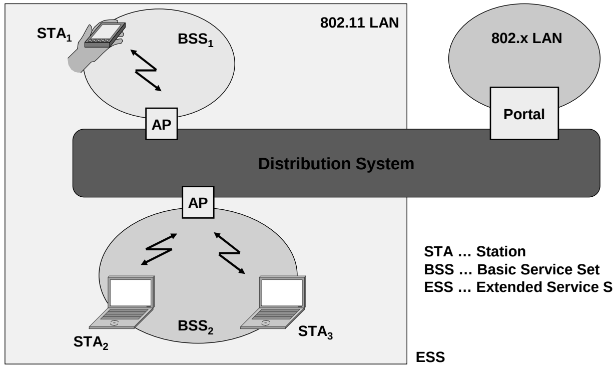
802.11 Standard

- **802.11 (oldest (1997), decommissioned, "legacy")**
  - 1 and 2 Mbit/s in the 2,4 GHz-Band
  - FHSS and DSSS
- **802.11a (2001, 2003)**
  - Up to 54 Mbit/s in the 5 GHz-Band
  - New OFDM technology
- **802.11b (first (1999) and most widespread)**
  - 5,5 and 11 Mbit/s in the 2,4 GHz-Band
  - Using only DSSS
- **802.11g (newest, 2003)**
  - 20+ Mbit/s in the 2,4 GHz-Band (b-compatibility)
  - Vendors decided to use 54 Mbit/s, OFDM

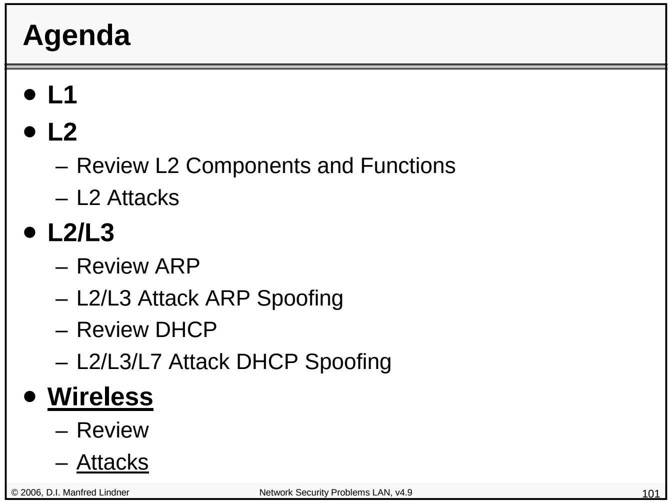
Ad-hoc Network



Infrastructure Network

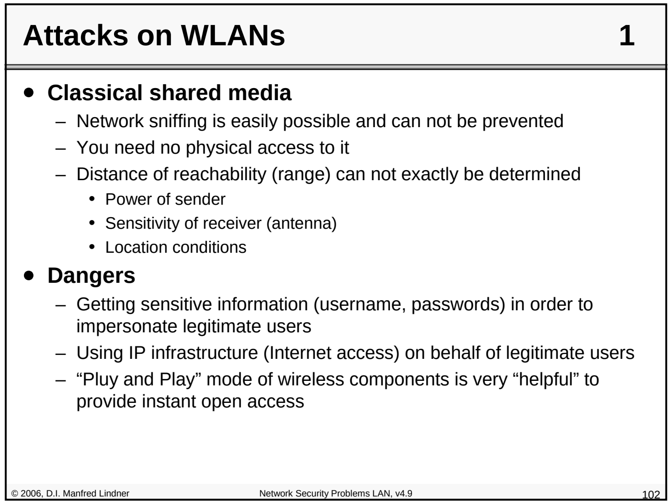


STA … Station
BSS … Basic Service Set
ESS … Extended Service Set



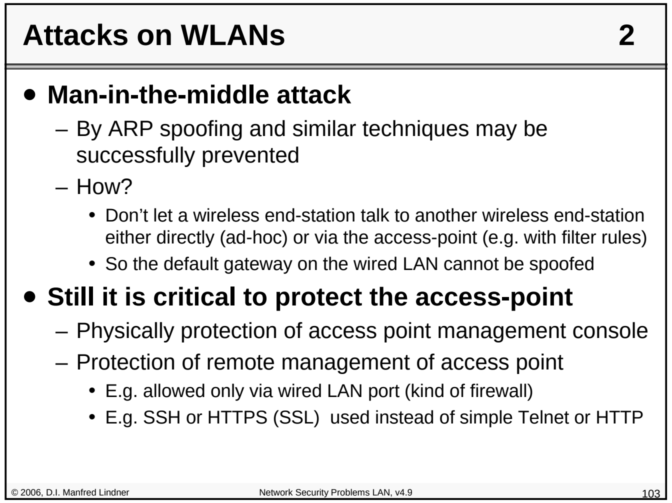
Agenda

- **L1**
- **L2**
  - – Review L2 Components and Functions
  - – L2 Attacks
- **L2/L3**
  - – Review ARP
  - – L2/L3 Attack ARP Spoofing
  - – Review DHCP
  - – L2/L3/L7 Attack DHCP Spoofing
- **Wireless**
  - – Review
  - – Attacks



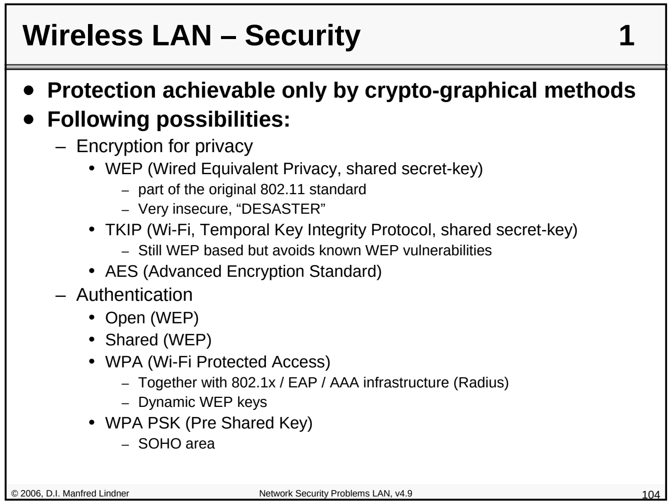
Attacks on WLANs 1

- **Classical shared media**
  - – Network sniffing is easily possible and can not be prevented
  - – You need no physical access to it
  - – Distance of reachability (range) can not exactly be determined
    - Power of sender
    - Sensitivity of receiver (antenna)
    - Location conditions
- **Dangers**
  - – Getting sensitive information (username, passwords) in order to impersonate legitimate users
  - – Using IP infrastructure (Internet access) on behalf of legitimate users
  - – “Pluy and Play” mode of wireless components is very “helpful” to provide instant open access



Attacks on WLANs 2

- **Man-in-the-middle attack**
  - – By ARP spoofing and similar techniques may be successfully prevented
  - – How?
    - Don’t let a wireless end-station talk to another wireless end-station either directly (ad-hoc) or via the access-point (e.g. with filter rules)
    - So the default gateway on the wired LAN cannot be spoofed
- **Still it is critical to protect the access-point**
  - – Physically protection of access point management console
  - – Protection of remote management of access point
    - E.g. allowed only via wired LAN port (kind of firewall)
    - E.g. SSH or HTTPS (SSL) used instead of simple Telnet or HTTP



Wireless LAN – Security 1

- **Protection achievable only by crypto-graphical methods**
- **Following possibilities:**
  - – Encryption for privacy
    - WEP (Wired Equivalent Privacy, shared secret-key)
      - – part of the original 802.11 standard
      - – Very insecure, “DESASTER”
    - TKIP (Wi-Fi, Temporal Key Integrity Protocol, shared secret-key)
      - – Still WEP based but avoids known WEP vulnerabilities
    - AES (Advanced Encryption Standard)
  - – Authentication
    - Open (WEP)
    - Shared (WEP)
    - WPA (Wi-Fi Protected Access)
      - – Together with 802.1x / EAP / AAA infrastructure (Radius)
      - – Dynamic WEP keys
    - WPA PSK (Pre Shared Key)
      - – SOHO area

Wireless LAN – Security 2

- **Following possibilities (cont.:**
  - Real strong solutions still on the way
    - IEEE 802.11i end of 2004 released
    - WPA-2
      - WPA2-Personal (PSK)
      - WPA2-Enterprise (EAP, AAA Server)
- **Even with crypto-graphical methods**
  - Discovery of WLAN infrastructure is possible
    - WLAN management frames
      - Beacons, Probe Request/Response
      - Authentication Request/Response
      - Association Request/Response
    - SSID, MAC in clear-text, L3 maybe secured
  - Denial of Service (DoS) is possible
    - E.g. high power RF signal generator

Wireless LAN – Security by VPN

- **VPN based on IPsec**
  - As alternative until final solution for wireless security is found
    - Either end-to-end or end-station to access-point
  - Maybe will complement or <u>replace</u> wireless security techniques
    - Question: How many different security techniques you want to configure and maintain in the IT/Network infrastructure of your company?

Wireless LAN - Sniffing

- **Discovery Tools**
  - NetStumbler (Windows)
    - http://netstumbler.com
    - MAC address
    - SSID
    - Access point name
    - Channel
    - Vendor
    - Security
  - Kismet (Linux)
    - http://www.kismetwireless.net
  - Dstumbler
    - http://www.openbsd.org -> bsd-airtools

Wireless LAN - WEP Cracking

- **Cracker Tools**
  - AirSnort (Windows, Linux)
    - http://sourceforge.net/projects/airsnort
  - WEPCrack (Linux)
    - http://sourceforge.net/projects/wepcrack