Secant

WHITE PAPER

IP ADDRESSING AND VLAN NUMBERING

Publication No. 100
Version: November 28, 2011

800.875.4222 • 6395 Technology Avenue, Kalamazoo, MI 49009 • secantcorp.com

IP Addressing and VLAN Numbering

OVERVIEW

This document provides a standard for the assignment of private IPv4 addresses and the numbering of VLANs within an organization's network. This standard should be adhered to in all locations where the Secant IP Addressing standard is already being used. For existing networks that do not currently use the Secant IP Addressing standard, the existing IP addressing scheme should be evaluated to determine if the network can be reconfigured to this standard. In most cases reconfiguring the network to use the Secant standard is highly recommended and can occur with relatively minimal downtime. This IP Addressing standard scheme can also be phased in over time in many cases depending on the existing IP addressing scheme and network configuration.

BACKGROUND

History

The IP Addressing standard was originally created in 1999 during the installation of a new WAN for a local school district. The existing standard is the result of over 12 years of continuous refinement with input from many Secant engineers. This IP addressing standard is now used by hundreds of different organizations.

Goals

The goals of the IP Addressing and VLAN Numbering standard are the following.

- Provide a consistent methodology of assigning private IP addresses
- Provide scalability and consistency
- Reduce the likelihood of IP address conflicts
- Reduce the need to maintain detailed IP address and VLAN assignment documentation
- Improve the readability of network traffic and statistics by specifying ranges for device types

BASE STANDARD

IP Address Ranges

This standard uses the 10.0.0.0/8 address block reserved for private IP addressing per RFC 1918. This is the only class A private address range, which provides the most scalability for private IP addressing. Most subnets in this standard use a class B, 16-bit mask, represented as subnet mask 255.255.0.0 or CIDR notation /16. Other subnets in this standard use a class C, 24-bit mask, represented as subnet mask 255.255.255.0 or CIDR notation /24.

The Backus–Naur Form (BNF) general format of most IP addresses in this standard is:

```
<IP Address> ::= "10." <VLAN-LOCATION> "." <DEVICE-CODE> "." <NODE>

    <VLAN-LOCATION> ::= 001 to 255
      <DEVICE-CODE> ::= 001 to 254
             <NODE> ::= 000 to 255
```

This standard also uses the 172.16.0.0/24 address block reserved for private IP addressing per RFC 1918. This subset of the class B private address range, is dedicated for VPN clients using a class C, 24-bit mask, represented as subnet mask 255.255.255.0 or CIDR notation /24.

The BNF general format of these IP addresses in this standard is:

```
<IP Address> ::= "172.16." <VLAN-LOCATION> "." <NODE>

    <VLAN-LOCATION> ::= 001 to 255
             <NODE> ::= 000 to 255
```

VLAN-LOCATION

VLAN-LOCATION codes range from 1 to 255 are used to represent physical locations, VLANs, and subnets. By convention the VLAN-LOCATION number in the IP address will match the layer 2 VLAN number where VLANs are implemented. VLAN-LOCATION codes are used to segment the network into smaller broadcast domains that are used for specific sites, functions, and traffic types.

Site VLAN-LOCATION Codes

Each physical site is assigned a base VLAN-LOCATION code which is also called the SITE-ID. The first site, which is typically the main office of an organization, is assigned 10. Site codes are incremented either by 5 or 10 depending on how many sites must be supported by the organization. Incrementing by 5 allows for 48 sites and by 10 allows for 24 sites. Incrementing by 10 is preferred whenever less than 25 sites are required.

At a physical site the network may be subnetted into several VLANs to reduce the number of hosts on a single subnet or to segregate specific traffic types. Each subnet should be limited to approximately 250 hosts to limit the amount of broadcast traffic on the subnet. In campus networks this is often accomplished by assigning a VLAN-LOCATION code to each wiring closet.

Additional VLAN-LOCATION codes are formed by incrementing the base VLAN-LOCATION code for the site. If physical locations are incremented by 10, then a total of 10 VLANs may be assigned per site. If incremented by 5, then 5 VLANs may be assigned per site. Occasionally a very large site will require more than 10 VLANs. These large sites should be assigned two adjacent ranges of VLAN-LOCATION codes, for example 10 to 29.

Example Location Code Assignments

The following table shows the VLANs for the first available range for a network that is incrementing each location number by 10:

VLAN-Location	Purpose	Notes
10	1st general VLAN	Base VLAN for site (also referred to as SITE-ID)
11	2nd general VLAN	
12	3rd general VLAN	
13	4th general VLAN	
14	5th general VLAN	
15	6th general VLAN	
16	7th general VLAN	
17	Facilities Traffic	Security cameras, access control, energy management
18	Wireless Traffic	Internal wireless network
19	VoIP Traffic	IP phones

The following table shows the VLANs for the first available range for a network that is incrementing each location number by 5:

VLAN-Location	Purpose	Notes
10	1st general VLAN	Base VLAN for site (also referred to as SITE-ID)
11	1st general VLAN	
12	Facilities Traffic	Security cameras, access control, energy management
13	Wireless Traffic	Internal wireless network
14	VoIP Traffic	IP phones

Function Subnets

The codes below are used to represent subnets reserved for functions rather than physical locations.

VLAN-Location	Purpose	Notes
001	Switch Management	10.1.LOC.NODE/16
002	External Traffic	Connection from core switch to firewall
003	Misc. Class C subnets	See Appendix section “Class C VLAN-LOCATION Codes”
004	Unassigned	
005	Virtual Desktops Class C subnets	See Appendix section “Class C VLAN-LOCATION Codes”
006	Servers	Servers - 1st range
007	Servers	Servers - 2nd range
008	Network Management	ILO, UPS, Environmental, KVM, Console ports
009	Servers	Server - 3rd range, core VoIP equipment
250	Ad-hoc networks	
251	Reserved for future use	
252	Reserved for future use	
253	Point-to-multipoint WAN	10.253.DESTINATION-LOC.NODE/24
254	Point-to-multipoint WAN	10.254.DESTINATION-LOC.NODE/30

Device Codes

DEVICE-CODEs range from 1 to 254 are assigned based on the type of device. Typically devices are assigned a static IP address, either by direct configuration of the device or using a DHCP reservation.

Device Code	Purpose	Notes
1 to 10	DHCP - Workstations, laptops, mobile devices	Supports 2,550 devices (10 x 255)
11 to 189	Unassigned	
190 to 198	Workstations with firewall exceptions	
199	Workstations - NATed	
200	Technician Workstation/Laptop	
201	Audio Visual - Control System	
202	Audio Visual - Control Panels	
203	Audio Visual - Flat Panel Display	
204	Audio Visual - Projectors	
205	Audio Visual - Amplifiers	
206	Audio Visual - Mixers	
207	Audio Visual - Switcher	
208	Audio Visual - Audio Processor, DSP	
209	Audio Visual - Video Equipment	
210	Audio Visual - Digital Signage Player	
211	Audio Visual - Reserved for future use	
212	Audio Visual - Reserved for future use	
213	Audio Visual - Streaming Video Encoder	
214	Audio Visual - Streaming TV Player	
215	Time card systems	
216	Environment sensors	Temperature, humidity, water, airflow

(CONTINUED)

Device Code	Purpose	Notes
217	Fibre Channel Switch	
218	iSCSI	
219	SAN Storage Management	
220	IP Clock	Clock Controllers .250 to .255
221	Access Control Systems and Security Alarms	
222	IP KVM	
223	Audio Visual Control Systems	DEPRECATED - Move to 201
224	Audio Visual Equipment	DEPRECATED - Move to 202-212
225	Network Management Console	Network polling/monitoring system, SNMP trap target
226	IP Telephony and Paging	Gateways, Fax devices, etc. Not phones
227	Energy management, building control	
228	Web Camera, Distance Learning Equipment	
229	Security Cameras and DVRs	
230	Printers, Copiers, Scanners	
231 to 238	Unassigned	
239	IP Controlled devices	
240	Servers - General	
241	LOM in 240 server	
242	Servers - Citrix/Terminal Services	
243	LOM in 244 server	
244	Servers - Site Specific	
245	LOM in 244 server	
246	Unassigned	
247	Hypervisor - Management	
248	Hypervisor - Migration (vMotion, etc.)	
249	Hypervisor - Host LOM	
250	UPS units, Managed power strips	
251	Wireless Controllers	
252	Switch - Layer 2	
253	Wireless Access Points	
254	Gateways (Router, firewall, layer 3 switch)	

Node

NODE is in the range 1 to 255 and provides the final octet of the IP address. Typically the first device is assigned 1 and next 2 and so on. Other strategies can be used and should be considered to organize NODE addresses in meaningful ways where it makes sense. For example, a group of devices on the first floor of a building might be placed in the 11-20 range, and the next group of devices on the second floor might be placed in the 21-30 range, etc.

ADDITIONAL SPECIFICATIONS

Class C VLAN-LOCATION Codes

The VLAN-LOCATION codes 3 and 5 are subnetted into 256 class C networks with a subnet mask of 255.255.255.0 or /24. This provides VLANs for special functions that do not require a larger class B range. There are many situations where it is desirable to allocate a VLAN to a small number of hosts to improve security or to segregate network traffic.

The BNF format of a Class C IP address is:

```
<Class C IP Address> ::= "10." <VLAN-LOCATION> "." <SUBNET-CODE> "." <NODE>
    <VLAN-LOCATION> ::= 003 | 005
      <SUBNET-CODE> ::= 000 to 254
             <NODE> ::= 001 to 254
```

Note that device codes are not available in class C networks, but since these networks are typically used for a single type of device they are less important. By convention the default gateway or router for any class C network is assigned the NODE value of 254. For example the gateway address for the 10.3.1.0/24 subnet will be 10.3.1.254.

Because VLAN-LOCATION codes 3 and 5 are subnetted into 256 ranges the typical rule for assigning VLAN numbers does not apply. VLAN numbers are based on a BASE-VLAN plus the SUBNET-CODE. The BASE-VLAN for 3 is 300 and the BASE-VLAN for 5 is 600.

VLAN-LOCATION Code 3 Subnets

Subnet Allocation for VLAN-LOCATION Code 003

SUBNET-CODE Range	VLAN Range	Purpose	Notes
0 to 9	300 to 309	Private DMZ or NAC	10 subnets for DMZ or NAC
10 to 59	310 to 359	Public Wireless	50 subnets for public wireless networks
60 to 79	360 to 379	iSCSI	20 iSCSI subnets, Targets at 10.3.x.1 to 99, Initiators at 10.3.x.100 to 253
80 to 99	380 to 399	Unassigned	
100 to 119	400 to 419	Microsoft NLB	20 subnets for MS NLB, Virtual Service at 10.3.xxx.1
120 to 254	420 to 554	Unassigned	

VLAN-LOCATION Code 5 Subnets

The VLAN-LOCATION code 5 has been defined to provide 255 class C networks for virtual desktops. This will accommodate more than 64,000 virtual desktops.

Subnet Allocation for VLAN-LOCATION Code 005

SUBNET-CODE Range	VLAN Range	Purpose	Notes
0 to 255	600 to 859	Virtual desktops	255 subnets for virtual desktops

External VLAN Numbering

VLAN numbers from 900 to 999 are used for external VLANs that are not routed to internal VLANs. For example a common use is to provide a layer-2 tunnel through a network to carry external traffic to the firewall's outside interface. The IP addresses on these VLANs will typically be public IPs or IP address ranges assigned by a third party.

External VLAN Numbers

VLAN-LOCATION	Purpose
900	Primary ISP connection
901 to 909	Secondary ISP connections
910 to 999	Connections to other entities

Switch Management IP Addresses

VLAN-LOCATION code 1 is reserved for network management. It is used to assign switch and other network management IP addresses. This isolates the management interface of the device from other network traffic. Network security can be enhanced by configuring an ACLs on the network's layer 3 routing devices to limit access to the management VLAN.

The BNF format of a switch management IP address is:

```
<SWITCH-MANAGEMENT-IP> ::= "10.1." <VLAN-LOCATION> "." <SWITCH-NUMBER>
<VLAN-LOCATION> ::= general VLAN for wiring closet where switch is installed
<SWITCH-NUMBER> ::= 10 to 19 for first closet, 20 to 29 for second closet, etc.
```

VPN Client IP Addressing

Clients connecting to a network using a VPN connection are assigned an IP address from a pool defined in the firewall. The private class B IP range 172.16.0.0/16 is used for this purpose. Each site specific VPN pool is assigned a /24 (class C) subnet from this range. The use of this unique range makes VPN user traffic easily distinguishable from internal network traffic during network analysis.

The BNF format of a VPN client IP address is:

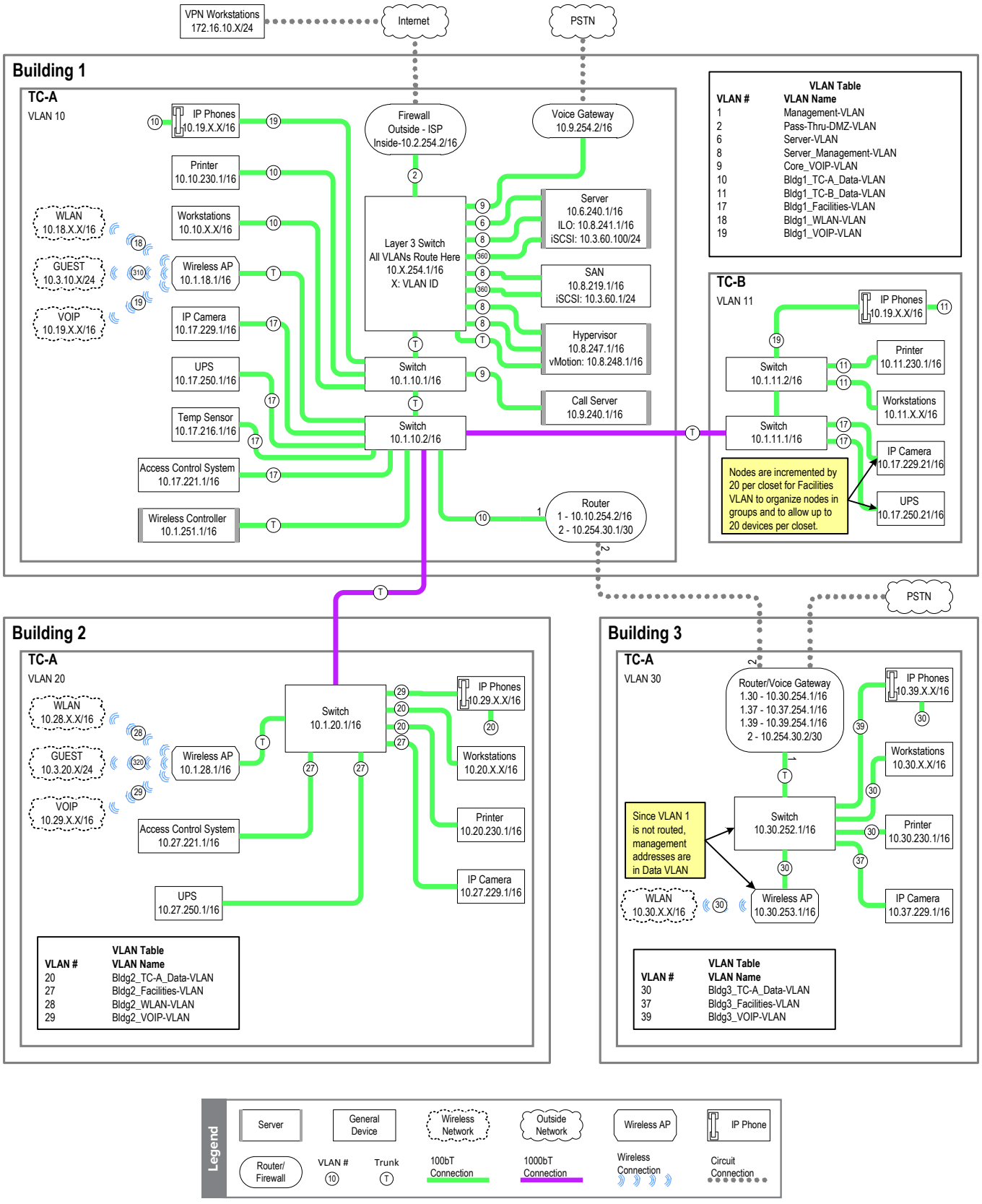
```
<VPN-CLIENT-ADDRESS> ::= "172.16." <SITE-ID> "." <NODE>
      <SITE ID> ::= first VLAN number for site where firewall is installed
         <NODE> ::= 000 to 255
```

Additional VPN Pools

Additional pools of VPN IP Addresses may be assigned to a site by incrementing the SITE-ID. For example third party contractors that VPN into site 10 may use the pool 172.16.11.0/24. Where the base SITE-ID of 10 has been incremented to 11.

SAMPLE NETWORK DIAGRAM

This network diagram illustrates the use of the IP Addressing and VLAN Numbering standard on a small multisite network.



800.875.4222 | SECANTCORP.COM